Cisco ME 3800X and ME 3600X Switch Command Reference

Cisco IOS Release 15.2(2)S
May 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-23401-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco ME 3800X and ME 3600X Switch Command Reference
© 2010—2012 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface xiii

Audience xiii

Purpose xiii

Conventions xiv

Related Publications xiv

Obtaining Documentation and Submitting a Service Request xv

CHAPTER 1 **Using the Command-Line Interface** 1-1

CLI Command Modes 1-1

User EXEC Mode 1-2

Privileged EXEC Mode 1-3

Global Configuration Mode 1-3

Interface Configuration Mode 1-4

VLAN Configuration Mode 1-4

Line Configuration Mode 1-4

CHAPTER 2 **Cisco ME 3800X and ME 3600X Switch Cisco IOS Commands** 2-1

action 2-1

aggregate interval 2-2

aggregate interval burst-cycles 2-3

alarm-contact 2-5

archive download-sw 2-7

archive tar 2-10

archive upload-sw 2-13

bandwidth 2-15

boot config-file 2-18

boot helper 2-19

boot helper-config-file 2-20

boot manual 2-21

boot private-config-file 2-22

boot system 2-23

channel-group 2-24

channel-protocol 2-27
class 2-28
class-map 2-30
clear ipc 2-32
clear lacp 2-33
clear logging onboard 2-34
clear mac address-table 2-35
clear pagp 2-37
clear rep counters 2-38
clear spanning-tree counters 2-39
conform-action 2-41
controller BITS input applique 2-43
controller BITS output applique 2-45
controller BITS shutdown 2-47
copy logging onboard module 2-48
define interface-range 2-50
delete 2-52
deny (MAC access-list configuration) 2-53
diagnostic schedule test 2-56
diagnostic start test 2-58
distribution 2-60
duplex 2-62
errdisable detect cause 2-64
errdisable recovery 2-66
ethernet evc 2-69
ethernet lmi 2-70
ethernet oam remote-failure 2-72
ethernet uni id 2-73
ethernet y1731 delay 2-74
ethernet y1731 loss 2-76
exceed-action 2-78
flowcontrol 2-80
frame consecutive 2-82
frame interval 2-83
frequency (IP SLA) 2-84

history interval **2-85**
hw-module module logging onboard **2-86**
interface port-channel **2-88**
interface range **2-90**
interface vlan **2-92**
ip access-group **2-94**
ip address **2-97**
ip igmp filter **2-99**
ip igmp max-groups **2-100**
ip igmp profile **2-102**
ip igmp snooping **2-104**
ip igmp snooping last-member-query-interval **2-105**
ip igmp snooping report-suppression **2-107**
ip igmp snooping tcn **2-109**
ip igmp snooping tcn flood **2-110**
ip igmp snooping vlan immediate-leave **2-111**
ip igmp snooping vlan mrouter **2-112**
ip igmp snooping vlan static **2-114**
ip sla **2-116**
ip sla reaction-configuration **2-118**
ip sla schedule **2-121**
ip ssh **2-124**
l2protocol **2-125**
l2 vfi **2-127**
lacp port-priority **2-129**
lacp system-priority **2-131**
location (global configuration) **2-133**
location (interface configuration) **2-135**
logging event **2-137**
logging file **2-138**
mac access-group **2-140**
mac access-list extended **2-142**
mac address-table aging-time **2-144**
mac address-table learning **2-146**
mac address-table move update **2-148**

mac address-table notification **2-150**
mac address-table static **2-152**
macro apply **2-154**
macro description **2-156**
macro global **2-157**
macro global description **2-159**
match (access-map configuration) **2-160**
match access-group **2-162**
match cos **2-163**
match discard-class **2-165**
match ip dscp **2-166**
match ip precedence **2-168**
match mpls experimental topmost **2-170**
match qos-group **2-172**
match vlan **2-174**
max-delay **2-176**
mdix auto **2-179**
mtu **2-181**
network-clock hold-off **2-182**
network-clock input-source **2-183**
network-clock revertive **2-185**
network-clock synchronization ssm option **2-186**
network-clock wait-to-restore **2-187**
network-clock-select **2-188**
network-clock-select hold-off timeout **2-189**
network-clock-select hold-timeout **2-190**
network-clock-select mode **2-192**
network-clock-select option **2-193**
network-clock-select output **2-194**
network-clock-select wait-to-restore-timeout **2-195**
oam protocol cfm svlan **2-196**
pagp learn-method **2-197**
pagp port-priority **2-199**
permit (MAC access-list configuration) **2-201**
police **2-204**

policy-map **2-208**
port-channel load-balance **2-211**
port-type **2-213**
priority **2-214**
ql-enabled rep-segment **2-216**
queue-limit **2-217**
random-detect **2-220**
random-detect cos **2-223**
random-detect cos-based **2-225**
random-detect dscp **2-226**
random-detect exponential-weighting-constant **2-229**
random-detect precedence **2-231**
rep admin vlan **2-233**
rep block port **2-234**
rep lsl-age-timer **2-237**
rep preempt delay **2-239**
rep preempt segment **2-241**
rep segment **2-242**
rep stcn **2-245**
reserved-only **2-247**
rmon collection stats **3-1**
service instance **3-2**
service password-recovery **3-4**
service-policy (interface and service-instance configuration modes) **3-6**
set cos **3-8**
set discard-class **3-10**
set dscp **3-11**
set mpls **3-13**
set network-clocks **3-15**
set precedence **3-17**
set qos-group **3-19**
setup **3-21**
shape average **3-24**
show access-lists **3-26**
show archive status **3-29**

show boot 3-30
show cable-diagnostics tdr 3-32
show class-map 3-34
show controllers bits 3-35
show controllers cpu-interface 3-36
show controllers ethernet-controller 3-38
show controllers utilization 3-43
show diagnostic 3-45
show env 3-49
show errdisable detect 3-52
show errdisable flap-values 3-54
show errdisable recovery 3-56
show etherchannel 3-58
show ethernet service evc 3-61
show flowcontrol 3-62
show interfaces 3-64
show interfaces counters 3-71
show interfaces rep 3-74
show interfaces transceiver 3-76
show inventory 3-79
show ip igmp profile 3-80
show ip igmp snooping 3-81
show ip igmp snooping groups 3-83
show ip igmp snooping mrouter 3-85
show ipc 3-86
show lacp 3-90
show location 3-94
show logging onboard 3-97
show mac access-group 3-101
show mac address-table 3-103
show mac address-table address 3-105
show mac address-table aging-time 3-107
show mac address-table bridge-domain 3-109
show mac address-table count 3-111
show mac address-table dynamic 3-113

show mac address-table interface 3-115
show mac address-table learning 3-117
show mac address-table move update 3-118
show mac address-table notification 3-120
show mac address-table static 3-122
show mac address-table vlan 3-124
show network-clocks 3-126
show pagp 3-128
show parser macro 3-130
show policy-map 3-132
show port-type 3-135
show rep topology 3-137
show spanning-tree 3-140
show storm-control 3-146
show udld 3-148
show version 3-150
show vfi 3-152
show vlan 3-154
show vlan access-map 3-157
show vlan filter 3-158
shutdown 4-1
shutdown vlan 4-2
snmp mib rep trap-rate 4-3
snmp-server enable traps 4-4
snmp-server host 4-8
snmp trap mac-notification change 4-12
spanning-tree bpdufilter 4-14
spanning-tree bpduguard 4-16
spanning-tree cost 4-18
spanning-tree etherchannel guard misconfig 4-20
spanning-tree extend system-id 4-22
spanning-tree guard 4-23
spanning-tree link-type 4-25
spanning-tree loopguard default 4-27
spanning-tree mode 4-29

spanning-tree mst configuration 4-30
spanning-tree mst cost 4-32
spanning-tree mst forward-time 4-34
spanning-tree mst hello-time 4-35
spanning-tree mst max-age 4-36
spanning-tree mst max-hops 4-37
spanning-tree mst port-priority 4-38
spanning-tree mst pre-standard 4-40
spanning-tree mst priority 4-41
spanning-tree mst root 4-42
spanning-tree port-priority 4-44
spanning-tree portfast (global configuration) 4-46
spanning-tree portfast (interface configuration) 4-48
spanning-tree vlan 4-50
speed 4-53
storm-control 4-55
switchport 4-58
switchport access vlan 4-60
switchport backup interface 4-62
switchport block 4-66
switchport host 4-68
switchport mode 4-69
switchport trunk 4-71
system env temperature threshold alert 4-73
test cable-diagnostics tdr 4-74
traceroute mac 4-75
traceroute mac ip 4-78
udld 4-80
udld port 4-82
udld reset 4-84
uni count 4-85
uni-vlan 4-87
violate-action 4-88
vlan 4-90
vlan access-map 4-93

vlan dot1q tag native 4-95
vlan filter 4-96
vpn id 4-97
xconnect 4-98

APPENDIX A

Cisco ME 3800X and ME 3600X Switch Boot Loader Commands A-1

arp A-2
boot A-3
cat A-5
copy A-6
delete A-7
dir A-8
flash_init A-10
format A-11
fsck A-12
help A-13
memory A-14
mgmt_clr A-15
mgmt_init A-16
mgmt_show A-17
mkdir A-18
more A-19
peek A-20
ping A-21
poke A-22
rename A-23
reset A-24
rmdir A-25
set A-26
set_param A-29
sleep A-30
type A-31
unset A-32
version A-34

APPENDIX B **Cisco ME 3800X and ME 3600X Switch Debug Commands** B-1

debug bridge-domain B-2
debug etherchannel B-3
debug ethernet service B-4
debug interface B-6
debug ip igmp filter B-7
debug ip igmp max-groups B-8
debug ip igmp snooping B-9
debug lacp B-10
debug mac-notification B-11
debug matm B-12
debug matm move B-13
debug network-clock B-14
debug nvram B-15
debug pagp B-16
debug pm B-17
debug rep B-19
debug qos B-20
debug spanning-tree B-21
debug spanning-tree bpdu B-23
debug spanning-tree bpdu-opt B-24
debug spanning-tree mstp B-25
debug spanning-tree switch B-27
debug spanning-tree vlan-shim B-29
debug sw-vlan B-31
debug sw-vlan ifs B-32
debug sw-vlan notification B-33
debug udld B-35
debug vfi B-37
debug vrrp B-38
debug xconnect B-39

APPENDIX C **Acknowledgments for Open-Source Software** C-1

INDEX

Preface

Audience

This guide is for the networking professional using the Cisco IOS command-line interface (CLI) to manage the Cisco Metro Ethernet (ME) 3800X and ME 3600X switches, hereafter referred to as *the switch*. Before using this guide, you should have experience working with the Cisco IOS commands and the switch software features. You should also have experience working with the concepts and terminology of Ethernet and local area networking.

Purpose

If you have a service support contract and order a software license or if you order a switch, you receive the universal software image, available in crypto an noncrypto versions. If you do not have a service support contract, such as a SMARTnet contract, download the image from Cisco.com.

The ME 3600X supports these licenses:

- Metro IP access is the universal image.
- Advanced Metro IP access license.
- 10 Gigabit Ethernet upgrade license.

The ME 3800X supports these licenses plus a scaled license that can be installed with any of these licenses to increase the supported values for that license, for example, more MAC addresses, VLANs, IPv4 routes, and so on. You must purchase the scaled license.

- Metro Ethernet services is the universal image.
- Metro IP services license.
- Metro Aggregation services license.

For differences in feature support for each license, see the software configuration guide.

To install a software image, see the switch release notes and the “Working with the Cisco IOS File System, Configuration Files, and Software Images” chapter in the software configuration guide.

This guide provides the information you need about the Layer 2 and Layer 3 commands that have been created or changed for use with the switch. For information about the standard Cisco IOS commands, see Master Index for Cisco IOS Software Release 12.4 from this page:
http://www.cisco.com/en/US/products/ps6350/tsd_products_support_series_home.html

This guide does not provide procedures for configuring your switch. For detailed configuration procedures, see the software configuration guide for this release.

This guide does not describe system messages you might encounter. For more information, see the system message guide for this release.

For the latest documentation updates, see the release notes for this release.

Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([ ]) means optional elements.
- Braces ( ) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes, cautions, and warnings use these conventions and symbols:

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Publications

These documents provide complete information about the switch and are available from these Cisco.com sites:

ME 3800X switch:
http://www.cisco.com/en/US/products/ps10965/tsd_products_support_series_home.html

ME 3600X switch:

http://www.cisco.com/en/US/products/ps10956/tsd_products_support_series_home.html

Note Before installing, configuring, or upgrading the switch, see these documents:

- For initial configuration information, see the "Configuring the Switch with the CLI-Based Setup Program" appendix in the hardware installation guide.
- For upgrading information, see the "Downloading Software" section in the release notes.

- *Release Notes for the Cisco ME 3800X and ME 3600X Switch*

Note See the release notes on Cisco.com for the latest information.

- *Cisco ME 3800X and ME 3600X Switch Software Configuration Guide*
- *Cisco ME 3800X and ME 3600X Switch Command Reference*
- *Cisco ME 3800X and ME 3600X System Message Guide*
- *Cisco ME 3800X and ME 3600X Switch Hardware Installation Guide*
- *Cisco ME 3800X and ME 3600X Switch Getting Started Guide*
- *Installation Notes for the Cisco ME 3800X and ME 3600X Switch Power-Supply and Fan Modules*
- *Regulatory Compliance and Safety Information for the Cisco ME 3800X and ME 3600X Switches*
- *Cisco Small Form-Factor Pluggable Modules Installation Notes*
- *Cisco CWDM GBIC and CWDM SFP Installation Notes*

These compatibility matrix documents are available from this Cisco.com site:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

- *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix*
- *Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix*
- *Cisco CWDM SFP Transceiver Compatibility Matrix*
- *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix*
- *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Using the Command-Line Interface

The Cisco Metro Ethernet (ME)3600 and 3800 Series switch is supported by Cisco IOS software. This chapter describes how to use the switch command-line interface (CLI) to configure software features.

For a complete description command descriptions, see these sections:

- For the configuration and monitoring commands that support these features, see Chapter 2, "Cisco ME 3800X and ME 3600X Switch Cisco IOS Commands."
- For information on the boot loader commands, see Appendix A, "Cisco ME 3800X and ME 3600X Switch Boot Loader Commands."
- For information on the **debug** commands, see Appendix B, "Cisco ME 3800X and ME 3600X Switch Debug Commands."
- For information on the **show platform** commands, see Appendix C, "Acknowledgments for Open-Source Software."
- For more information on Cisco IOS Release 12.2, see the *Cisco IOS Release 12.2 Command Summary.*

For task-oriented configuration steps, see the software configuration guide for this release.

In this document, unless otherwise specified, IP refers to IP version 4 (IPv4).

CLI Command Modes

This section describes the CLI command mode structure. Command modes support specific Cisco IOS commands. For example, the **interface** *interface-id* command only works when entered in global configuration mode.

These are the main command modes for the switch:

- User EXEC
- Privileged EXEC
- Global configuration
- Interface configuration
- VLAN configuration
- Line configuration

Table 1-1 lists the main command modes, how to access each mode, the prompt you see in that mode, and how to exit that mode. The prompts listed use the default name *Switch*.

Table 1-1 Command Modes Summary

Command Mode	Access Method	Prompt	Exit or Access Next Mode
User EXEC	This is the first level of access. (For the switch) Change terminal settings, perform basic tasks, and list system information.	`Switch>`	Enter the **logout** command. To enter privileged EXEC mode, enter the **enable** command.
Privileged EXEC	From user EXEC mode, enter the **enable** command.	`Switch#`	To exit to user EXEC mode, enter the **disable** command. To enter global configuration mode, enter the **configure** command.
Global configuration	From privileged EXEC mode, enter the **configure** command.	`Switch(config)#`	To exit to privileged EXEC mode, enter the **exit** or **end** command, or press **Ctrl-Z**. To enter interface configuration mode, enter the **interface** configuration command.
Interface configuration	From global configuration mode, specify an interface by entering the **interface** command followed by an interface identification.	`Switch(config-if)#`	To exit to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**. To exit to global configuration mode, enter the **exit** command.
VLAN configuration	In global configuration mode, enter the **vlan** *vlan-id* command.	`Switch(config-vlan)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.
Line configuration	From global configuration mode, specify a line by entering the **line** command.	`Switch(config-line)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.

User EXEC Mode

After you access the device, you are automatically in user EXEC command mode. The EXEC commands available at the user level are a subset of those available at the privileged level. In general, use the user EXEC commands to temporarily change terminal settings, perform basic tests, and list system information.

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (**?**) at the prompt.

```
Switch> ?
```

Privileged EXEC Mode

Because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use. The privileged command set includes those commands contained in user EXEC mode, as well as the **configure** privileged EXEC command through which you access the remaining command modes.

If your system administrator has set a password, you are prompted to enter it before being granted access to privileged EXEC mode. The password does not appear on the screen and is case sensitive.

The privileged EXEC mode prompt is the device name followed by the pound sign (#).

```
Switch#
```

Enter the **enable** command to access privileged EXEC mode:

```
Switch> enable
Switch#
```

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (**?**) at the prompt.

```
Switch# ?
```

To return to user EXEC mode, enter the **disable** privileged EXEC command.

Global Configuration Mode

Global configuration commands apply to features that affect the device as a whole. Use the **configure** privileged EXEC command to enter global configuration mode. The default is to enter commands from the management console.

When you enter the **configure** command, a message prompts you for the source of the configuration commands:

```
Switch# configure
Configuring from terminal, memory, or network [terminal]?
```

You can specify either the terminal or nonvolatile RAM (NVRAM) as the source of configuration commands.

This example shows you how to access global configuration mode:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (**?**) at the prompt.

```
Switch(config)# ?
```

To exit global configuration command mode and to return to privileged EXEC mode, enter the **end** or **exit** command, or press **Ctrl-Z**.

Interface Configuration Mode

Interface configuration commands modify the operation of the interface. Interface configuration commands always follow a global configuration command, which defines the interface type.

Use the **interface** *interface-id* command to access interface configuration mode. The new prompt means interface configuration mode.

```
Switch(config-if)#
```

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (**?**) at the prompt.

```
Switch(config-if)# ?
```

To exit interface configuration mode and to return to global configuration mode, enter the **exit** command. To exit interface configuration mode and to return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.

VLAN Configuration Mode

Use this mode to configure normal-range VLANs (VLAN IDs 1 to 1005) or extended-range VLANs (VLAN IDs 1006 to 4094). The VLAN configuration is saved in the running configuration file, and you can save it to the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command. The configurations of VLAN IDs 1 to 1005 are saved in the VLAN database. The extended-range VLAN configurations are not saved in the VLAN database.

Enter the **vlan** *vlan-id* global configuration command to access VLAN configuration mode:

```
Switch(config)# vlan 2000
Switch(config-vlan)#
```

To display a comprehensive list of available commands, enter a question mark (**?**) at the prompt.

```
Switch(config-vlan)# ?
```

For extended-range VLANs, many characteristics are not configurable and must remain at the default setting.

To return to global configuration mode, enter **exit**; to return to privileged EXEC mode, enter **end**. All the commands except **shutdown** take effect when you exit config-vlan mode.

Line Configuration Mode

Line configuration commands modify the operation of a terminal line. Line configuration commands always follow a line command, which defines a line number. Use these commands to change terminal parameter settings line-by-line or for a range of lines.

Use the **line vty** *line_number* [*ending_line_number*] command to enter line configuration mode. The new prompt means line configuration mode. The following example shows how to enter line configuration mode for virtual terminal line 7:

```
Switch(config)# line vty 0 7
```

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (**?**) at the prompt.

```
Switch(config-line)# ?
```

To exit line configuration mode and to return to global configuration mode, use the **exit** command. To exit line configuration mode and to return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.

CHAPTER 2

Cisco ME 3800X and ME 3600X Switch Cisco IOS Commands

action

To set the action for the VLAN access map entry, use the **action** command in access-map configuration mode. To set the action to the default value, which is to forward, use the **no** form of this command.

action {**drop** | **forward**}

no action

Syntax Description

drop	Drops the packet when the specified conditions are matched.
forward	Forwards the packet when the specified conditions are matched.

Defaults

The default action is to forward packets.

Command Modes

Access-map configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

If the action is **drop**, you should define the access map, including configuring any access control list (ACL) names in match clauses, before applying the map to a VLAN, or all packets could be dropped.

In access-map configuration mode, use the **match** access-map configuration command to define the match conditions for a VLAN map. Use the **action** command to set the action that occurs when a packet matches the conditions.

The drop and forward parameters are not used in the **no** form of the command.

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

Examples

This example shows how to identify and apply a VLAN access map *vmap4* to VLANs 5 and 6 that causes the VLAN to forward an IP packet if the packet matches the conditions defined in access list *al2*:

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan filter vmap4 vlan-list 5-6
```

Related Commands

Command	Description
access-list {**deny** | **permit**}	Configures a standard numbered ACL.
ip access-list	Creates a named access list.
mac access-list extended	Creates a named MAC address access list.
match (access-map configuration)	Defines the match conditions for a VLAN map.
show vlan access-map	Displays the VLAN access maps created on the switch.
vlan access-map	Creates a VLAN access map.

aggregate interval

To configure an aggregate interval for an IP Service Level Agreements (SLAs) Metro-Ethernet 3.0 (Y.1731) operation, use the aggregate interval command in IP SLA Y.1731 delay or IP SLA Y.1731 loss configuration mode. To return to the default, use the no form of this command.

aggregate interval *seconds*

no aggregate interval

Syntax Description

seconds	Length of time in seconds. The range is from 1 to 65535. The default is 900.

Defaults

The default aggregate interval is 900 seconds.

Command Modes

P SLA Y.1731 delay configuration (config-sla-y1731-delay)

IP SLA Y.1731 loss configuration (config-sla-y1731-loss)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

An aggregate interval is the length of time during which the performance measurements are conducted and the results stored. Use this command to change the number of intervals for a delay, delay variation, or frame loss operation from the default (900 seconds) to the specified value.

The aggregate interval value must be less than the life value of the IP SLAs schedule. The default life value for an IP SLAs schedule or IP SLAs multioperation group scheduler configuration is 3600 seconds.

Examples

The following example shows how to configure a single-ended IP SLAs Ethernet delay operation with an aggregate interval of 1500 seconds:

```
Switch(config)# ip sla 10
Switch(config-ip-sla)# ethernet y7131 delay dmm domain xxx evc yyy mpid 101 cos 3 source
mpid 100
Switch(config-sla-y1731-delay)# aggregate interval 1500
Switch(config-sla-y1731-delay)#
```

Related Commands

Command	Description
distribution	Configures statistics distributions for an IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) operation.
history interval	Sets the number of statistics distributions kept during the lifetime of an IP SLAs Metro Ethernet 3.0 (ITU-T Y.1731) operation.
ip sla group schedule	Configures multioperation scheduling for IP SLAs operations.
ip sla schedule	Configures the scheduling parameters for a single IP SLAs operation.
show ip sla statistics	Displays the current operational status and statistics of all IP SLAs operations or a specified operation.

aggregate interval burst-cycles

To configure an aggregate interval for burst-cycles for an IP Service Level Agreements (SLAs) Metro-Ethernet 3.0 (Y.1731) operation, use the aggregate interval command in IP SLA Y.1731 synthetic loss configuration mode. To return to the default, use the no form of this command.

aggregate {interval} burst-cycles *seconds*

no aggregate interval

Syntax Description

burst-cycles	Specifies the number of burst-cycles
seconds	Length of time in seconds. The range is from 1 to 65535. The default is 900.

Defaults

The default aggregate interval is 1 seconds.

Command Modes

IP SLA Y.1731 loss configuration (config-sla-y1731-loss)

Command History

Release	Modification
15.2(4)S1	This command was introduced.

Usage Guidelines

An aggregate interval burst-cycle is the number of burst cycles on which the performance measurements are conducted and teh resultes stored. Use this command to change the number of intervals for a frame loss operation from the default (1 second) to the specified value.

The aggregate interval value must be less than the life value of the IP SLAs schedule. The default life value for an IP SLAs schedule or IP SLAs multioperation group scheduler configuration is 3600 seconds.

Examples

The following example shows how to configure a single-ended IP SLAs Ethernet delay operation with an aggregate interval of 6 seconds:

```
Switch(config)# ip sla 10
Switch(config-ip-sla)# ethernet y7131 loss slm burst domain xxx evc yyy mpid 101 cos 3
source mpid 100
Switch(config-sla-y1731-delay)# aggregate interval burst-cycles 6
Switch(config-sla-y1731-delay)#
```

Related Commands

Command	Description
distribution	Configures statistics distributions for an IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) operation.
history interval	Sets the number of statistics distributions kept during the lifetime of an IP SLAs Metro Ethernet 3.0 (ITU-T Y.1731) operation.
ip sla group schedule	Configures multioperation scheduling for IP SLAs operations.
ip sla schedule	Configures the scheduling parameters for a single IP SLAs operation.
show ip sla statistics	Displays the current operational status and statistics of all IP SLAs operations or a specified operation.

alarm-contact

To configure triggers and severity levels for external alarms, use the **alarm-contact** command in global configuration mode. To remove the configuration, use the **no** form of this command.

alarm-contact {*contact-number* {**description** *string* | **severity** {**critical** | **major** | **minor**} | **trigger** {**closed** | **open**}} | **all** {**severity** {**critical** | **major** | **minor**} | **trigger** {**closed** | **open**}}

no alarm-contact {*contact-number* {**description** | **severity** | **trigger**} | **all** {**severity** | **trigger**}

contact-number	Configures a specific alarm contact number. The range is 1 to 4.
description *string*	Adds a description for the alarm contact number. The description string can be up to 80 alphanumeric characters in length and is included in the system message generated when the alarm is triggered.
all	Configures all alarm contacts.
severity	Sets the severity level that is set when the alarm is triggered. The severity is included in the alarm notification. Entering **no alarm-contact severity** sets the severity to minor.
critical	Sets severity level as critical.
major	Sets severity level as major.
minor	Sets severity level as minor.
trigger	Sets the state that triggers the alarm, whether the connected circuit is open or closed. Entering **no alarm-contact trigger** sets the trigger to closed.
closed	Specifies that the alarm is triggered when the contact is closed.
open	Specifies that the alarm is triggered when the contact is open.

Defaults

No alarms are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **no alarm-contact** *contact-number* **description** sets the description to an empty string.

The **no alarm-contact** {*contact-number* | **all**} **severity** sets the alarm-contact severity to minor.

The **no alarm-contact** {*contact-number* | **all**} **trigger** sets the external alarm-contact trigger to closed.

You can verify your settings by entering the **show env alarm-contact** or the **show running-config** privileged EXEC command.

Examples

This example shows how to configure alarm contact number 1 to report a critical alarm when the contact is open.

```
Switch(config)# alarm-contact 1 description main_lab_door
Switch(config)# alarm-contact 1 severity critical
Switch(config)# alarm-contact 1 trigger open
Dec  4 10:34:09.049: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_ASSERT: Alarm asserted:
main_lab_door

Switch# show env alarm-contact
ALARM CONTACT 1
   Status:      asserted
   Description: main_lab_door
   Severity:    critical
   Trigger:     open
```

This example shows how to configure clear alarm contact number 1 and the show command outputs.

```
Switch(config)# no alarm-contact 1 description
Dec  4 10:39:33.621: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_CLEAR: Alarm cleared:
main_lab_door Dec  4 10:39:33.621: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_ASSERT: Alarm
asserted: external alarm contact 1

Switch(config)# no alarm-contact 1 severity
Dec  4 10:39:46.774: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_CLEAR: Alarm cleared: external
alarm contact 1 Dec  4 10:39:46.774: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_ASSERT: Alarm
asserted: external alarm contact 1

Switch(config)# no alarm-contact 1 trigger open
Dec  4 10:39:56.547: %PLATFORM_ENV-1-EXTERNAL_ALARM_CONTACT_CLEAR: Alarm cleared: external
alarm contact 1
Switch(config)# end

Switch# show env alarm-contact
ALARM CONTACT 1
   Status:      not asserted
   Description: external alarm contact 1
   Severity:    minor
   Trigger:     closed
ALARM CONTACT 2
   Status:      not asserted
   Description: external alarm contact 2
   Severity:    minor
   Trigger:     closed
ALARM CONTACT 3
   Status:      not asserted
   Description: external alarm contact 3
   Severity:    minor
   Trigger:     closed
ALARM CONTACT 4
   Status:      not asserted
   Description: external alarm contact 4
   Severity:    minor
   Trigger:     closed
```

Related Commands

Command	Description
show env alarm-contact	Displays the alarm setting and status for the switch.

archive download-sw

To download a new image from a TFTP server to the switch and to overwrite or keep the existing image, use the **archive download-sw** command in privileged EXEC mode.

archive download-sw {**/force-reload** | **/imageonly** | **/leave-old-sw** | **/no-set-boot** | **/no-version-check** | **/overwrite** | **/reload** | **/safe**} *source-url*

Syntax Description

/force-reload	Unconditionally forces a system reload after successfully downloading the software image.
/imageonly	Downloads only the software image but not the HTML files associated with the embedded device manager. The HTML files for the existing version are deleted only if the existing version is being overwritten or removed.
/leave-old-sw	Keeps the old software version after a successful download.
/no-set-boot	Specified to not alter the setting of the BOOT environment variable to point to the new software image after it is successfully downloaded.
/no-version-check	Downloads the software image without checking to prevent installing an incompatible image.
/overwrite	Overwrites the software image in flash memory with the downloaded one.
/reload	Reloads the system after successfully downloading the image unless the configuration has been changed and not been saved.
/safe	Keeps the current software image; do not delete it to make room for the new software image before the new image is downloaded. The current image is deleted after the download.
source-url	The source URL alias for a local or network file system. These options are supported: • The syntax for the local flash file system: **flash:** • The syntax for the FTP: **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***image-name***.tar** • The syntax for an HTTP server: **http://**[[*username***:***password*]**@**]{*hostname* | *host-ip*}[**/***directory*]**/***image-name***.tar** • The syntax for a secure HTTP server: **https://**[[*username***:***password*]**@**]{*hostname* | *host-ip*}[**/***directory*]**/***image-name***.tar** • The syntax for the Remote Copy Protocol (RCP): **rcp:**[[**//***username***@***location*]**/***directory*]**/***image-name***.tar** • The syntax for the TFTP: **tftp:**[[**//***location*]**/***directory*]**/***image-name***.tar** The *image-name***.tar** is the software image to download and install on the switch.

Defaults

The current software image is not overwritten with the downloaded image.

Both the software image and HTML files are downloaded.

The new image is downloaded to the flash: file system.

The BOOT environment variable is changed to point to the new software image on the flash: file system.

Image names are case sensitive; the image file is provided in tar format.

Compatibility of the version on the image to be downloaded is checked.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **/imageonly** option removes the HTML files for the existing image if the existing image is being removed or replaced. Only the Cisco IOS image (without the HTML files) is downloaded.

Using the **/safe** or **/leave-old-sw** option can cause the new image download to fail if there is insufficient flash memory. If leaving the software in place prevents the new image from fitting in flash memory due to space constraints, an error results.

If you used the **/leave-old-sw** option and did not overwrite the old image when you downloaded the new one, you can remove the old image by using the **delete** privileged EXEC command. For more information, see the **delete** command.

Note Use the **/no-version-check** option with care. This option allows an image to be downloaded without first confirming that it is not incompatible with the switch.

Use the **/overwrite** option to overwrite the image on the flash device with the downloaded one.

If you specify the command *without* the **/overwrite** option, the download algorithm verifies that the new image is not the same as the one on the switch flash device. If the images are the same, the download does not occur. If the images are different, the old image is deleted, and the new one is downloaded.

After downloading a new image, enter the **reload** privileged EXEC command to begin using the new image, or specify the **/reload** or **/force-reload** option in the **archive download-sw** command.

Examples

This example shows how to download a new image from a TFTP server at 172.20.129.10 and overwrite the image on the switch:

```
Switch# archive download-sw /overwrite tftp://172.20.129.10/test-image.tar
```

This example shows how to download only the software image from a TFTP server at 172.20.129.10 to the switch:

```
Switch# archive download-sw /imageonly tftp://172.20.129.10/test-image.tar
```

This example shows how to keep the old software version after a successful download:

```
Switch# archive download-sw /leave-old-sw tftp://172.20.129.10/test-image.tar
```

Related Commands

Command	Description
archive tar	Creates a tar file, lists the files in a tar file, or extracts the files from a tar file.
archive upload-sw	Uploads an existing image on the switch to a server.
delete	Deletes a file or directory on the flash memory device.

archive tar

To create a tar file, list files in a tar file, or extract the files from a tar file, use the **archive tar** command in privileged EXEC mode.

archive tar {**/create** *destination-url* **flash:/***file-url*} | {**/table** *source-url*} | {**/xtract** *source-url* **flash:/***file-url* [*dir/file...*]}

Syntax Description

/create *destination-url* **flash:/***file-url*	Creates a new tar file on the local or network file system. For *destination-url, specify t*he destination URL alias for the local or network file system and the name of the tar file to create. These options are supported: • The syntax for the local flash filesystem: **flash:** • The syntax for the FTP: **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar** • The syntax for the Remote Copy Protocol (RCP) is: **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar** • The syntax for the TFTP: **tftp:**[[**//***location*]**/***directory*]**/***tar-filename***.tar** The *tar-filename***.tar** is the tar file to be created. For **flash:/***file-url, specify t*he location on the local flash file system from which the new tar file is created. An optional list of files or directories within the source directory can be specified to write to the new tar file. If none are specified, all files and directories at this level are written to the newly created tar file.
/table *source-url*	Displays the contents of an existing tar file to the screen. For *source-url*, specify the source URL alias for the local or network file system. These options are supported: • The syntax for the local flash file system: **flash:** • The syntax for the FTP: **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar** • The syntax for the RCP: **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar** • The syntax for the TFTP: **tftp:**[[**//***location*]**/***directory*]**/***tar-filename***.tar** The *tar-filename***.tar** is the tar file to display.

/xtract *source-url* **flash:**/*file-url* [*dir/file...*]	Extracts files from a tar file to the local file system. For *source-url*, specify *t*he source URL alias for the local file system. These options are supported: • The syntax for the local flash file system: **flash:** • The syntax for the FTP: **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar** • The syntax for the RCP: **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar** • The syntax for the TFTP: **tftp:**[[**//***location*]**/***directory*]**/***tar-filename***.tar** The *tar-filename***.tar** is the tar file from which to extract. For **flash:/***file-url* [*dir/file...*], specify *t*he location on the local flash file system into which the tar file is extracted. Use the *dir/file...* option to specify an optional list of files or directories within the tar file to be extracted. If none are specified, all files and directories are extracted.

Defaults

None

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Image names are case sensitive.

Examples

This example shows how to create a tar file. The command writes the contents of the *new-configs* directory on the local flash device to a file named *saved.tar* on the TFTP server at 172.20.10.30:

```
Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs
```

This example shows how to display the contents of the file that is in flash memory. The contents of the tar file appear on the screen:

```
Switch# archive tar /table flash:image_name-mz.122-release.tar
info (219 bytes)
image_name-mz.122-release/(directory)
image_name-mz.122-release(610856 bytes)
image_name-mz.122-release/info (219 bytes)
info.ver (219 bytes)
```

This example shows how to display only the *html* directory and its contents:

```
Switch# archive tar /table flash:image_name-mz.122-release.tar
image_name-mz.122-release/html
image_name-mz.122-release/html/ (directory)
image_name-mz.122-release/html/const.htm (556 bytes)
image_name-mz.122-release/html/xhome.htm (9373 bytes)
image_name-mz.122-release/html/menu.css (1654 bytes)
<output truncated>
```

This example shows how to extract the contents of a tar file on the TFTP server at 172.20.10.30. This command extracts just the *new-configs* directory into the root directory on the local flash file system. The remaining files in the *saved.tar* file are ignored.

```
Switch# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/ new-configs
```

Related Commands

Command	Description
archive download-sw	Downloads a new image from a TFTP server to the switch.
archive upload-sw	Uploads an existing image on the switch to a server.

archive upload-sw

To upload an existing switch image to a server, use the **archive upload-sw** command in privileged EXEC mode.

archive upload-sw [**/version** *version_string*] **destination-url**

Syntax Description

/version *version_string*	(Optional) Specifies the specific version string of the image to be uploaded.
destination-url	The destination URL alias for a local or network file system. These options are supported: • The syntax for the local flash file system: **flash:** • The syntax for the FTP: **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***image-name***.tar** • The syntax for the Remote Copy Protocol (RCP): **rcp:**[[**//***username@location*]**/***directory*]**/***image-name***.tar** • **T**he syntax for the TFTP: **tftp:**[[**//***location*]**/***directory*]**/***image-name***.tar** The *image-name***.tar** is the name of software image to be stored on the server.

Defaults

Uploads the currently running image from the flash: file system.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use the upload feature only if the HTML files associated with the embedded device manager have been installed with the existing image.

The files are uploaded in this sequence: the Cisco IOS image, the HTML files, and info. After these files are uploaded, the software creates the tar file.

Image names are case sensitive.

Examples

This example shows how to upload the currently running image to a TFTP server at 172.20.140.2:

```
Switch# archive upload-sw tftp://172.20.140.2/test-image.tar
```

Related Commands

Command	Description
archive download-sw	Downloads a new image to the switch.
archive tar	Creates a tar file, lists the files in a tar file, or extracts the files from a tar file.

bandwidth

To configure class-based weighted fair queuing (CBWFQ) by setting the output bandwidth for a policy-map class, use the **bandwidth** command in policy-map class configuration mode. To remove the bandwidth setting for the class, use the **no** form of this command.

bandwidth {*rate* | **percent** *value* | **remaining percent** *value*}

no bandwidth [*rate* | **percent** *value* | **remaining percent** *value*]

Syntax Description

rate	Sets the bandwidth rate for the class in kilobits per second (kbps). The range is from 1 to 10000000 Kb/s **Note** The total guaranteed bandwidth cannot exceed the total available rate or total bandwidth of the interface.
percent *value*	Sets the bandwidth for the class as a percent of the parent policy peak information rate (PIR) or shape value. The range is from 1 to 100 percent. **Note** The total guaranteed bandwidth cannot exceed the total available rate or total bandwidth of the interface.
remaining percent *value*	Sets the bandwidth for the class as a percent of the remaining bandwidth. The range is from 0 to 100 percent. **Note** he total guaranteed bandwidth cannot exceed the total available rate or total bandwidth of the interface.

Defaults

No bandwidth is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You use the **bandwidth** policy-map class command to control output traffic. The **bandwidth** command specifies the bandwidth for traffic in that class. CBWFQ derives the weight for packets belonging to the class from the bandwidth allocated to the class and uses the weight to ensure that the queue for that class is serviced fairly. Bandwidth settings are not supported in input policy maps.

- Configuring bandwidth for a class of traffic as an absolute rate (kilobits per second) or a percentage of total bandwidth represents the minimum bandwidth guarantee (CIR) for that traffic class.
- You cannot configure bandwidth as an absolute rate or a percentage of total bandwidth when **priority** is configured for another class in the output policy. However, you can configure CIR, PIR, and EIR bandwidth independently for a class so can use the **bandwidth**, **bandwidth remaining**, and **shape average** commands at the same time within a class.

- Configuring bandwidth as a percentage of *remaining* bandwidth determines the portion of the excess bandwidth of the target that is allocated to the class. This means that the class is allocated bandwidth only if there is excess bandwidth on the target, and if there is no minimum bandwidth guarantee for this traffic class. By default the total excess bandwidth is divided equally among the classes.
- You cannot configure bandwidth as percentage of remaining bandwidth when **priority** is configured for another class in the output policy map.

When you configure bandwidth in an output policy, you must specify the same units in each bandwidth configuration; that is, all absolute values (rates) or percentages.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how to allocate 25 percent of the total available bandwidth to the traffic class defined by the class map:

```
Switch(config)# policy-map gold_policy
Switch(config-pmap)# class out_class-1
Switch(config-pmap-c)# bandwidth percent 25
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output gold_policy
Switch(config-if)# exit
```

This example shows how to set the precedence of output queues by setting bandwidth in kilobits per second. The classes *outclass1*, *outclass2*, and *outclass3* and **class-default** get a minimum of 40000, 20000, 10000, and 10000 kb/s. Any excess bandwidth is divided among the classes in the same proportion as the CIR rate.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth 40000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth 10000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth 10000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

This example shows how to allocate the excess bandwidth among queues by configuring bandwidth for a traffic class as a percentage of remaining bandwidth. The class *outclass1* is given priority queue treatment. The other classes are configured to get percentages of the excess bandwidth if any remains after servicing the priority queue: *outclass2* is configured to get 50 percent, *outclass3* to get 20 percent, and the class **class-default** to get the remaining 30 percent.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
```

```
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays quality of service (QoS) policy maps.

boot config-file

To specify the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration, use the **boot config-file** command in global configuration mode. To return to the default setting, use the **no** form of this command.

boot config-file *file-name*

no boot config-file

Syntax Description

file-name	The name of the configuration file.

Defaults

The default configuration file is flash:config.text.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

This command changes the setting of the CONFIG_FILE environment variable. For more information, see Appendix A, "Cisco ME 3800X and ME 3600X Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	Displays the settings of the boot environment variables.

boot helper

To dynamically load files during boot loader initialization to extend or patch the functionality of the boot loader, use the **boot helper** command in global configuration mode. To return to the default, use the **no** form of this command.

boot helper *filesystem***:/***file-url* ...

no boot helper

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	The path (directory) and a list of loadable files to dynamically load during loader initialization. Separate each image name with a semicolon.

Defaults

No helper files are loaded.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

This variable is used only for internal development and testing.

Filenames and directory names are case sensitive.

This command changes the setting of the HELPER environment variable. For more information, see Appendix A, "Cisco ME 3800X and ME 3600X Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	Displays the settings of the boot environment variables.

boot helper-config-file

To specify the name of the configuration file to be used by the Cisco IOS helper image, use the **boot helper-config-file** command in global configuration mode. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of Cisco IOS that are loaded. To return to the default setting, use the **no** form of this command.

boot helper-config-file *filename*

no boot helper-config file

Syntax Description

file-name	The helper configuration file to load.

Defaults

No helper configuration file is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

This variable is used only for internal development and testing.

Filenames and directory names are case sensitive.

This command changes the setting of the HELPER_CONFIG_FILE environment variable. For more information, see Appendix A, "Cisco ME 3800X and ME 3600X Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	Displays the settings of the boot environment variables.

boot manual

To enable manually booting the switch during the next boot cycle, use the **boot manual** command in global configuration mode. To return to the default setting, use the **no** form of this command.

boot manual

no boot manual

Syntax Description

This command has no arguments or keywords.

Defaults

Manual booting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The next time you reboot the system, the switch is in boot loader mode, which is shown by the *switch:* prompt. To boot the system, use the **boot** boot loader command, and specify the name of the bootable image.

This command changes the setting of the MANUAL_BOOT environment variable. For more information, see Appendix A, "Cisco ME 3800X and ME 3600X Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	Displays the settings of the boot environment variables.

boot private-config-file

To specify the filename that Cisco IOS uses to read and write a nonvolatile copy of the private configuration, use the **boot private-config-file** command in global configuration mode. To return to the default setting, use the **no** form of this command.

boot private-config-file *filename*

no boot private-config-file

Syntax Description

filename	The name of the private configuration file.

Defaults

The default configuration file is *private-config*.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Filenames are case sensitive.

Examples

This example shows how to specify the name of the private configuration file to be *pconfig*:

```
Switch(config)# boot private-config-file pconfig
```

Related Commands

Command	Description
show boot	Displays the settings of the boot environment variables.

boot system

To specify the Cisco IOS image to load during the next boot cycle, use the **boot system** command in global configuration mode. To return to the default setting, use the **no** form of this command.

boot system *filesystem:/file-url* ...

no boot system

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	The path (directory) and name of a bootable image. Separate image names with a semicolon.

Defaults

The switch attempts to automatically boot the system by using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable image it can by performing a recursive, depth-first search throughout the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you are using the **archive download-sw** privileged EXEC command to maintain system images, you never need to use the **boot system** command. The **boot system** command is automatically manipulated to load the downloaded image.

This command changes the setting of the BOOT environment variable. For more information, see Appendix A, "Cisco ME 3800X and ME 3600X Switch Boot Loader Commands."

Related Commands

Command	Description
show boot	Displays the settings of the boot environment variables.

channel-group

To assign an Ethernet port to an EtherChannel group, use the **channel-group** command in interface configuration mode. To remove an Ethernet port from an EtherChannel group, use the **no** form of this command.

channel-group *channel-group-number* **mode** {**active** | **auto** [**non-silent**] | **desirable** [**non-silent**] | **on** | **passive**}

no channel-group

PAgP modes:
channel-group *channel-group-number* **mode** {**auto** [**non-silent**] | **desirable** [**non-silent**]}

LACP modes:
channel-group *channel-group-number* **mode** {**active** | **passive**}

On mode:
channel-group *channel-group-number* **mode on**

Syntax Description

channel-group-number	Specifies the channel group number. The range is 1 to 26.
mode	Specifies the EtherChannel mode.
active	Unconditionally enables LACP Active mode places a port into a negotiating state in which the port initiates negotiations with other ports by sending LACP packets. A channel is formed with another port group in either the active or passive mode.
auto	Enables the PAgP only if a PAgP device is detected. Auto mode places a port into a passive negotiating state in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. A channel is formed only with another port group in desirable mode. When **auto** is enabled, silent operation is the default.
desirable	Unconditionally enables PAgP. Desirable mode places a port into an active negotiating state in which the port starts negotiations with other ports by sending PAgP packets. A channel is formed with another port group in either the desirable or auto mode. When **desirable** is enabled, silent operation is the default.
non-silent	(Optional) Use in PAgP mode with the **auto** or **desirable** keyword when traffic is expected from the other device.
on	Enables **on** mode. In **on** mode, a usable EtherChannel exists only when both connected port groups are in the **on** mode.
passive	Enables LACP only if a LACP device is detected. Passive mode places a port into a negotiating state in which the port responds to LACP packets it receives but does not initiate LACP packet negotiation. A channel is formed only with another port group in active mode.

Defaults

No channel groups are assigned.

No mode is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

For Layer 2 EtherChannels, you do not have to create a port-channel interface first by using the **interface port-channel** global configuration command before assigning a physical port to a channel group. Instead, you can use the **channel-group** interface configuration command. It automatically creates the port-channel interface when the channel group gets its first physical port if the logical interface is not already created. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number,* or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

If the port is a UNI or an ENI, you must use the **no shutdown** interface configuration command to enable it before using the **channel-group** command. UNIs and ENIs are disabled by default. NNIs are enabled by default.

You do not have to disable the IP address that is assigned to a physical port that is part of a channel group, but we strongly recommend that you do so.

You create Layer 3 port channels by using the **interface port-channel** command followed by the **no switchport** interface configuration command. You should manually configure the port-channel logical interface before putting the interface into the channel group.

After you configure an EtherChannel, configuration changes that you make on the port-channel interface apply to all the physical ports assigned to the port-channel interface. Configuration changes applied to the physical port affect only the port where you apply the configuration. To change the parameters of all ports in an EtherChannel, apply configuration commands to the port-channel interface, for example, spanning-tree commands or commands to configure a Layer 2 EtherChannel as a trunk.

If you do not specify **non-silent** with the **auto** or **desirable** mode, silent is assumed. The silent mode is used when the switch is connected to a device that is not PAgP-capable and seldom, if ever, sends packets. A example of a silent partner is a file server or a packet analyzer that is not generating traffic. In this case, running PAgP on a physical port prevents that port from ever becoming operational. However, it allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission. Both ends of the link cannot be set to silent.

In the **on** mode, an EtherChannel exists only when a port group in the **on** mode is connected to another port group in the **on** mode.

Caution You should exercise care when setting the mode to **on** (manual configuration). All ports configured in the **on** mode are bundled in the same group and are forced to have similar characteristics. If the group is misconfigured, packet loss or spanning-tree loops might occur.

Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same switch. Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.

If you set the protocol by using the **channel-protocol** interface configuration command, the setting is not overridden by the **channel-group** interface configuration command.

For a complete list of configuration guidelines, see the "Configuring EtherChannels" chapter in the software configuration guide for this release.

Caution Do not enable Layer 3 addresses on the physical EtherChannel ports. Do not assign bridge groups on the physical EtherChannel ports because it creates loops.

You can verify your settings by entering the **show running-config** privileged EXEC command.

Examples

This example shows how to configure an EtherChannel. It assigns two static-access ports in VLAN 10 to channel 5 with the PAgP mode **desirable**:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable
Switch(config-if-range)# end
```

This example shows how to configure an EtherChannel. It assigns two static-access ports in VLAN 10 to channel 5 with the LACP mode **active**:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

Related Commands

Command	Description
channel-protocol	Restricts the protocol used on a port to manage channeling.
interface port-channel	Accesses or creates the port channel.
show etherchannel	Displays EtherChannel information for a channel.
show lacp	Displays LACP channel-group information.
show pagp	Displays PAgP channel-group information.
show running-config	Displays the operating configuration.

channel-protocol

To restrict the protocol used on a port to manage channeling, use the **channel-protocol** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

channel-protocol {**lacp** | **pagp**}

no channel-protocol

Syntax Description

lacp	Configures an EtherChannel with the Link Aggregation Control Protocol (LACP).
pagp	Configures an EtherChannel with the Port Aggregation Protocol (PAgP).

Defaults

No protocol is assigned to the EtherChannel.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use the **channel-protocol** command only to restrict a channel to LACP or PAgP. If you set the protocol by using the **channel-protocol** command, the setting is not overridden by the **channel-group** interface configuration command.

You must use the **channel-group** interface configuration command to configure the EtherChannel parameters. The **channel-group** command also can set the mode for the EtherChannel.

You cannot enable both the PAgP and LACP modes on an EtherChannel group.

PAgP and LACP are not compatible; both ends of a channel must use the same protocol.

You can verify your settings by entering the **show etherchannel** [*channel-group-number*] **protocol** privileged EXEC command.

Examples

This example shows how to specify LACP as the protocol that manages the EtherChannel:

```
Switch(config-if)# channel-protocol lacp
```

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group.
show etherchannel protocol	Displays protocol information the EtherChannel.

class

To specify the name of the class whose policy you want to create or to change or to specify the system default class before you configure a policy and to enter policy-map class configuration mode, use the **class** command in policy-map configuration mode. To remove the class from a policy map, use the **no** form of this command.

class {*class-map-name*| **class-default**}

no class {*class-map-name*| **class-default**}

Syntax Description

class-map-name	Name of a class map created by using the **class-map** global configuration command.
class-default	The system default class. This class matches all unclassified traffic. You cannot create or delete the default class.

Defaults

No policy map classes are defined.

Command Modes

Policy-map configuration

Command History

Release	Modification
12.252)EY	This command was introduced.

Usage Guidelines

Before using the **class** *class-map-name* command in policy-map configuration mode, you must create the class by using the **class-map** *class-map-name* global configuration command. The class **class-default** is the class to which traffic is directed if that traffic does not match any of the match criteria in the configured class maps.

Use the **policy-map** global configuration command to identify the policy map and to enter policy-map configuration mode. After specifying a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map.

You attach the policy map to a port by using the **service-policy** interface configuration command.

After entering the **class** command, you enter policy-map class configuration mode, and these configuration commands are available:

- **bandwidth**: specifies the bandwidth allocated for a class belonging to a policy map. For more information, see the **bandwidth** command.
- **exit**: exits policy-map class configuration mode and returns to policy-map configuration mode.
- **no**: returns a command to its default setting.
- **police**: defines an individual policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information, see the **police** and policy-map class commands.

- **priority**: sets the strict scheduling priority for this class or, when used with the **police** keyword, sets priority with police. For more information, see the **priority** policy-map class command.
- **queue-limit**: sets the queue maximum threshold for Weighted Tail Drop (WTD). For more information, see the **queue-limit** command.
- **service-policy**: configures a QoS service policy to attach to a parent policy map for an input or output policy. For more information, see the **set cos** command.
- **set**: specifies a value to be assigned to the classified traffic. For more information, see the **set** commands.
- **shape average**: specifies the average traffic shaping rate. For more information, see the **shape average** command.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how to create a policy map called *policy1,* define a class *class1*, and enter policy-map class configuration mode to set a criterion for the class.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays QoS policy maps.
show policy-map interface [interface-id]	Displays policy maps configured on the specified interface or on all interfaces.

class-map

To create a class map to be used for matching packets to a specified criteria and to enter class-map configuration mode, use the **class-map** command in global configuration mode. To delete an existing class map, use the **no** form of this command.

class-map [**match-all** | **match-any**] *class-map-name*

no class-map [**match-all** | **match-any**] *class-map-name*

Syntax Description

match-all	(Optional) Performs a logical-AND of all matching statements under this class map. Packets must meet all of the match criteria.
match-any	(Optional) Performs a logical-OR of the matching statements under this class map. Packets must meet one or more of the match criteria.
class-map-name	Name of the class map.

Defaults

No class maps are defined.

If neither the **match-all** or the **match-any** keyword is specified, the default is **match-all**.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use this command to specify the name of the class for which you want to create or to modify class-map match criteria and to enter class-map configuration mode.

The switch supports a maximum of 4000 unique class maps.

You use the **class-map** command and class-map configuration mode to define packet classification as part of a globally named service policy applied on a per-port basis. When you configure a class map, you can use one or more **match** commands to specify match criteria. Packets arriving at either the input or output interface (determined by how you configure the **service-policy** interface configuration command) are checked against the class-map match criteria to determine if the packet belongs to that class.

A **match-all** class map means that the packet must match all entries and can have no other match statements. The **match-all** keyword is supported only for outer VLAN and inner VLAN, or outer CoS and inner CoS matches for 802.1Q tunneling (QinQ) packets. The **match-all** keyword is rejected for all other mutually exclusive match criteria.

After you are in class-map configuration mode, these configuration commands are available:

- **description**: describes the class map (up to 200 characters). The **show class-map** privileged EXEC command displays the description and the name of the class map.
- **exit**: exits QoS class-map configuration mode.

- **match**: configures classification criteria. For more information, see the **match** class-map configuration commands.
- **no**: removes a match statement from a class map.

You can verify your settings by entering the **show class-map** privileged EXEC command.

Examples

This example shows how to configure the class map called *class1*. By default, the class map is **match-all** and therefore can contain no other match criteria.

```
Switch(config)# class-map class1
Switch(config-cmap)# exit
```

This example shows how to configure a match-any class map with one match criterion, which is an access list called *103*. This class map (matching an ACL) is supported only in an input policy map.

```
Switch(config)# class-map class2
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
```

This example shows how to delete the class map ***class1***:

```
Switch(config)# no class-map class1
```

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
match access-group	Configures the match criteria for a class map on the basis of the specified access control list (ACL)
match cos	Configures the match criteria for a class map on the basis of the Layer 2 class of service (CoS) marking,
match discard-class	Configures a discard behavior identifier.
match ip dscp	Configures the match criteria for a class map on the basis of a specific IPv4 Differentiated Service Code Point (DSCP) value.
match ip precedence	Configures the match criteria for a class map on the basis of IPv4 precedence values.
match mpls experimental topmost	Match MPLS experimental value on the topmost label.
match qos-group	Configures the match criteria for a class map on the basis of a specific quality of service (QoS) group value.
match vlan	Configures the match criteria for a class map in the parent policy of a hierarchical policy map based on a VLAN ID or range of VLAN IDs.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show class-map	Displays QoS class maps.

clear ipc

To clear Interprocess Communications Protocol (IPC) statistics, use the **clear ipc** command in privileged EXEC mode.

clear ipc {queue-statistics | statistics}

Syntax Description

queue-statistics	Clears the IPC queue statistics.
statistics	Clears the IPC statistics.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can clear all statistics by using the **clear ipc statistics** command, or you can clear only the queue statistics by using the **clear ipc queue-statistics** command.

You can verify that the statistics were deleted by entering the **show ipc rpc** or the **show ipc session** privileged EXEC command.

Examples

This example shows how to clear all statistics:

```
Switch# clear ipc statistics
```

This example shows how to clear only the queue statistics:

```
Switch# clear ipc queue-statistics
```

Related Commands

Command	Description
show ipc {**rpc** | **session**}	Displays the IPC multicast routing statistics.

clear lacp

To clear Link Aggregation Control Protocol (LACP) channel-group counters, use the **clear lacp** command in privileged EXEC mode.

clear lacp {*channel-group-number* **counters** | **counters**}

Syntax Description

channel-group-number	(Optional) Channel group number. The range is 1 to 26.
counters	Clears traffic counters.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can clear all counters by using the **clear lacp counters** command, or you can clear only the counters for the specified channel group by using the **clear lacp** *channel-group-number* **counters** command.

You can verify that the information was deleted by entering the **show lacp counters** or the **show lacp 4 counters** privileged EXEC command.

Examples

This example shows how to clear all channel-group information:

```
Switch# clear lacp counters
```

This example shows how to clear LACP traffic counters for group 4:

```
Switch# clear lacp 4 counters
```

Related Commands

Command	Description
show lacp	Displays LACP channel-group information.

clear logging onboard

To clear all the on-board failure logging (OBFL) data except for the uptime and CLI-command information stored in the flash memory, use the **clear logging onboard** command in privileged EXEC mode.

clear logging onboard [**module** {*slot-number* | **all**}]

Syntax Description

module {*slot-number* | **all**}	(Optional) The slot number is always 1 and is not relevant for the ME-3400E. Entering **clear logging onboard module 1** or **clear logging onboard all** has the same result as entering **clear logging onboard**.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

We recommend that you keep OBFL enabled and do not clear the data stored in the flash memory.

You can verify that the information was cleared by entering the **show logging onboard onboard** privileged EXEC command.

Examples

These examples show how to clear all the OBFL information except for the uptime and CLI-command information:

```
Switch# clear logging onboard
Clear logging onboard buffer [confirm]
PID: ME-3400E-24TS-M   , VID: 03 , SN: FOC1225U4CY

Switch# clear logging onboard module all
Clear logging onboard buffer [confirm]
PID: ME-3400E-24TS-M   , VID: 03 , SN: FOC1225U4CY
```

Related Commands

Command	Description
hw-module module logging onboard	Enables OBFL.
show logging onboard	Displays OBFL information.

clear mac address-table

To delete a specific dynamic address from the MAC address table, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN, use the **clear mac address-table** command in privileged EXEC mode. This command also clears the MAC address notification global counters.

clear mac address-table {**dynamic** [**address** *mac-addr* | **bridge-domain** *number3* | **interface** *interface-id* | **vlan** *vlan-id*] | **move update** | **notification**}

Syntax Description

dynamic	Deletes all dynamic MAC addresses.
dynamic address *mac-addr*	(Optional) Deletes the specified dynamic MAC address.
dynamic bridge-domain *number*	(Optional) Deletes all dynamic MAC addresses for the bridge domain. The domain number range from 1 to 8000.
dynamic interface *interface-id*	(Optional) Deletes all dynamic MAC addresses on the specified physical port or port channel.
dynamic vlan *vlan-id*	(Optional) Deletes all dynamic MAC addresses for the specified VLAN. The range is 1 to 4096.
move update	Clears the MAC address move update related counters.
notification	Clears the notifications in the history table and reset the counters.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to remove a specific MAC address from the dynamic address table:

```
Switch# clear mac address-table dynamic address 0008.0070.0007
```

You can verify that any information was deleted by entering the **show mac address-table** privileged EXEC command.

This example shows how to clear the mac address-table move update related counters.

```
Switch# clear mac address-table move update
```

You can verify that the information was cleared by entering the **show mac address-table move update** privileged EXEC command.

Related Commands

Command	Description
mac address-table notification	Enables the MAC address notification feature.
show mac address-table	Displays the MAC address table static and dynamic entries.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
snmp trap mac-notification change	Enables the Simple Network Management Protocol (SNMP) MAC address notification trap on a specific interface.
mac address-table move update	Configures MAC address-table move update on the switch.
show mac address-table move update	Displays the MAC address-table move update information on the switch.

clear pagp

To clear Port Aggregation Protocol (PAgP) channel-group information, use the **clear pagp** command in privileged EXEC mode.

clear pagp {*channel-group-number* **counters** | **counters**}

Syntax Description

channel-group-number	(Optional) Channel group number. The range is 1 to 48.
counters	Clear traffic counters.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can clear all counters by using the **clear pagp counters** command, or you can clear only the counters for the specified channel group by using the **clear pagp** *channel-group-number* **counters** command.

You can verify that information was deleted by entering the **show pagp** privileged EXEC command.

Examples

This example shows how to clear all channel-group information:

```
Switch# clear pagp counters
```

This example shows how to clear PAgP traffic counters for group 10:

```
Switch# clear pagp 10 counters
```

Related Commands

Command	Description
show pagp	Displays PAgP channel-group information.

clear rep counters

To clear Resilient Ethernet Protocol (REP) counters for the specified interface or all interfaces, use the **clear rep counters** command in privileged EXEC mode.

clear rep counters [**interface** *interface-id*]

Syntax Description

interface *interface-id*	(Optional) Specifies a REP interface whose counters should be cleared.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can clear all REP counters by using the **clear rep counters** command, or you can clear only the counters for the interface by using the **clear rep counters interface** *interface-id* command.

When you enter the **clear rep counters** command, only the counters visible in the output of the **show interface rep detail** command are cleared. SNMP visible counters are not cleared as they are read-only.

You can verify that REP information was deleted by entering the **show interfaces rep detail** privileged EXEC command.

Examples

This example shows how to clear all REP counters for all REP interfaces:

```
Switch# clear rep counters
```

Related Commands

Command	Description
show interfaces rep detail	Displays detailed REP configuration and status information.

clear spanning-tree counters

To clear the spanning-tree counters or to restart the protocol migration processor on all spanning-tree interfaces or on the specified interface, use the **clear spanning-tree counters** command in privileged EXEC mode.

clear spanning-tree {counters [**interface** *interface-id*] **| detected-protocols** [**interface** *interface-id*]}

Syntax Description

counters	Clears the spanning-tree counters.
detected-protocols	Restarts the protocol migration process (force the renegotiation with neighboring switches).
interface *interface-id*	(Optional) Clears all spanning-tree counters or restart the protocol migration process on the specified interface. Valid interfaces include physical interfaces, VLANs, and spanning-tree port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 26.

Defaults

No default is defined.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If the *interface-id* is not specified, spanning-tree counters are cleared for all STP ports or the protocol migration is restarted on all STP ports.

A switch running the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol or the Multiple Spanning Tree Protocol (MSTP) supports a built-in protocol migration mechanism that enables it to interoperate with legacy IEEE 802.1D switches. If a rapid-PVST+ switch or an MSTP switch receives a legacy IEEE 802.1D configuration bridge protocol data unit (BPDU) with the protocol version set to 0, it sends only IEEE 802.1D BPDUs on that port. A multiple spanning-tree (MST) switch can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (Version 3) associated with a different region, or a rapid spanning-tree (RST) BPDU (Version 2).

However, the switch does not automatically revert to the rapid-PVST+ or the MSTP mode if it no longer receives IEEE 802.1D BPDUs. It cannot learn whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. Use the **clear spanning-tree detected-protocols** command in this situation.

Examples

This example shows how to clear spanning-tree counters for all STP ports:

```
Switch# clear spanning-tree counters
```

This example shows how to restart the protocol migration process on a port:

```
Switch# clear spanning-tree detected-protocols interface gigabitethernet0/1
```

Related Commands

Command	Description
show spanning-tree	Displays spanning-tree state information.
spanning-tree link-type	Overrides the default link-type setting and enables rapid spanning-tree transitions to the forwarding state.

conform-action

To set actions for a policy-map class for packets that conform to the committed information rate (CIR), use the **conform-action** command in policy-map class police configuration mode. To cancel the action or to return to the default action, use the **no** form of this command.

conform-action {**drop** | **set-cos-transmit** *new cos-value* | **set-discard-class-transmit** *new discard-value* | **set-dscp-transmit** *new dscp-value* | **set-mpls-exp-imposition-transmit** *new-imposition-exp-value* | **set-mpls-exp-topmost transmit** *new-topmost-exp-value* | **set-prec-transmit value** *new prec-value* | **set-qos-transmit value** *new qos-value*| **transmit**}

no conform-action {**drop** | **set-cos-transmit** *new cos-value* | **set-discard-class-transmit** *new discard-value* | **set-dscp-transmit** *new dscp-value* | **set-mpls-exp-imposition-transmit** *new-imposition-exp-value* | **set-mpls-exp-topmost transmit** *new-topmost-exp-value* | **set-prec-transmit value** *new prec-value* | **set-qos-transmit value** *new qos-value*| **transmit**}

Syntax Description

drop	Drops the packet.
set-cos-transmit *new-cos-value*	Sets a new class of service (CoS) value for the packet and send the packet. The range for the new CoS value is 0 to 7.
set-discard-class-transmit *new discard-value*	Sets a new discard-class value for the packet and send the packet. The range for the value is 0 to 7.
set-dscp-transmit *new-dscp-value*	Sets a new Differentiated Services Code Point (DSCP) value for the packet and send the packet. The range for the new DCSP value is 0 to 63.
set-mpls-exp-imposition transmit *new-imposition-exp-value*	Sets an MPLS label using the new MPLS EXP value at tag imposition, and send the packet. The range is 0 to 7.
set-mpls-exp-topmost transmit *new-topmost-exp-value*	Sets an MPLS label using the new MPLS EXP value for the topmost (outer) MPLS label, and send the packet. The range is 0 to 7.
set-prec-transmit *new-precedence-value*	Sets a new IP precedence value for the packet and send the packet. The range for the new IP precedence value is 0 to 7.
set-qos-transmit *qos-group-value*	Sets a new quality of service (QoS) group value for the packet and send the packet. The range for the new QoS value is 0 to 99.
transmit	(Optional) Sends the packet unmodified.

Defaults

The default conform action is to send the packet.

Command Modes

Policy-map class police configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You configure conform actions for packets when the packet rate conforms to the configured conform burst.

The switch also supports simultaneously marking multiple QoS parameters for the same class and configuring conform-action, exceed-action, and violate-action marking.

Access policy-map class police configuration mode by entering the **police** policy-map class command. See the **police** policy-map class configuration command for more information.

Use this command to set one or more conform actions for a traffic class.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how to configure the conform action of a policy map to set a new CoS value to 3 and send the packet.

```
Switch(config)# class-map cos-4
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class cos-4
Switch(config-pmap-c)# police cir 5000000 pir 8000000
Switch(config-pmap-c-police)# conform-action set-cos-transmit 3
Switch(config-pmap-c-police)# end
```

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
exceed-action	Defines the action to take on traffic that exceeds the CIR.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
police	Defines a policer for classified traffic.
show policy-map	Displays QoS policy maps.
violate-action	Defines the action to take on traffic with a rate greater than the conform rate plus the exceed burst.

controller BITS input applique

To configure the Building Integrated Timing Supply (BITS) clock input link type and characteristics, use the **controller BITS input applique** command in global configuration mode. To remove the configuration, use the **no** form of this command.

controller BITS input applique E1{**2048KHz | framing** {**fas_crc4 | fas_nocrc | |mfas_crc4 | mfas_nocre**} **linecode** {**ami | hdb3**}

controller BITS input applique T1 framing {**d4 | esf**} **linecode** {**ami | b8zs**}

no controller BITS input applique

Syntax Description

E1 2048 KHz	Specifies an EI timing signal input of 2048 KHz.
E1 framing	Specifies an EI signal input and specify the framing mode as one of these options: • **fas_crc4**—FASCRC4 • **fas_nocrc**—FAS • **mfas_crc4**—MFASCRC4 • **mfas_nocre**—MFAS
linecode (EI)	Selects the E1 line coding: • **ami—**AMI encoding • **hdb3—**HDB3 encoding
T1 framing	Specifies a T1 (1.544 MHz) signal input and specify the framing mode as one of these options: • **d4—**D4 • **esf**—Extended Superframe
linecode (T1)	Selects the T1 line coding: • **ami—**AMI encoding • **b8zs—**B8ZS encoding

Defaults

The default input timing is E1.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to set the input line type to T1 with ESF framing and B8ZS line coding:

```
Switch(config)# controller BITS input applique T1 framing esf linecode ami b8zs
Switch(config)# exit
```

Related Commands

Command	Description
show controller bits	Displays BITS configuration for the switch.

controller BITS output applique

To configure the Building Integrated Timing Supply (BITS) clock output link type and characteristics, use the **controller BITS output applique** command in global configuration mode. To remove the configuration, use the **no** form of this command.

controller BITS output applique E1{**2048KHz | framing** {**fas_crc4 | fas_nocrc | |mfas_crc4 | mfas_nocre**} **linecode** {**ami | hdb3**}

controller BITS output applique T1 framing {**d4 | esf**} **linecode** {**ami | b8zs**} **line-build-out** {**0-133ft | 133-266ft | 266-399ft | 399-533ft | 533-655ft**}

no controller BITS output applique

Syntax Description

E1 2048 KHz	Specifies an EI timing signal input of 2048 KHz.
E1 framing	Specifies an EI signal input and specify the framing mode as one of these options: • **fas_crc4**—FASCRC4 • **fas_nocrc**—FAS • **mfas_crc4**—MFASCRC4 • **mfas_nocre**—MFAS
linecode (E1)	Selects the E1 line coding: • **ami—**AMI encoding • **hdb3—**HDB3 encoding
T1 framing	Specifies a T1 (1.544 MHz) signal input and specify the framing mode as one of these options: • **d4—**D4 • **esf**—Extended Superframe
linecode (T1)	Selects the T1 line coding: • **ami—**AMI encoding • **b8zs—**B8ZS encoding
line-build-out	Selects a line length: • **0-133ft** • **133-266ft** • **266-399ft** • **399-533ft** • **533-655ft**

Command Default

The default output timing is E1.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to set the output line type to T1 with ESF framing and B8ZS line coding and a line buildout of 0 to 133 feet:

```
Switch(config)# controller BITS output applique T1 framing esf linecode ami b8zs
build-out 0-133ft
Switch(config)# exit
```

Related Commands

Command	Description
show controller bits	Displays BITS configuration for the switch.

controller BITS shutdown

To shut down the Building Integrated Timing Supply (BITS) clock controller, use the **controller BITS shutdown** command in global configuration mode.To reverse the shutdown, use the **no** form of this command.

controller BITS shutdown

no controller BITS shutdown

Syntax Description

This command has no keywords.

Defaults

The clock controller is on by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to shut down the BITS controller:

```
Switch(config)# controller BITS shutdown
Switch(config)# exit
```

Related Commands

Command	Description
show controller bits	Displays BITS configuration for the switch.

copy logging onboard module

To copy on-board failure logging (OBFL) data to the local network or a specific file system, use the **copy logging onboard module** command in privileged EXEC mode.

copy logging onboard module [*slot-number*] *destination*

Syntax Description

slot-number	(Optional) The slot number is always 1 and is not relevant for the ME-3400E.
destination	Specifies the location on the local network or file system to which the system messages are copied. For *destination,* specify the destination on the local or network file system and the filename. These options are supported: • The syntax for the local flash file system: **flash:/***filename* • The syntax for the FTP: **ftp://***username***:***password*@*host*/*filename* • The syntax for an HTTP server: **http://**[[*username***:***password*]@]{*hostname* | *host-ip*}[/*directory*]/*filename* • The syntax for the null file system: **null:/***filename* • The syntax for the NVRAM: **nvram:/***filename* • The syntax for the Remote Copy Protocol (RCP): **rcp://***username*@*host*/*filename* • The syntax for the switch file system: **system:***filename* • The syntax for the TFTP: **tftp:**[[//*location*]/*directory*]/*filename* • The syntax for the temporary file system: **tmpsys:/***filename*

Defaults

This command has no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

For information about OBFL, see the global configuration command.

Examples

This example shows how to copy the OBFL data messages to the *obfl_file* file on the flash file system:

```
Switch# copy logging onboard module flash:obfl_file
OBFL copy successful
```

Related Commands

Command	Description
hw-module module logging onboard	Enables OBFL.
show logging onboard	Displays OBFL information.

define interface-range

To create an interface-range macro, use the **define interface-range** command in global configuration mode. To delete the defined macro, use the **no** form of this command.

define interface-range *macro-name interface-range*

no define interface-range *macro-name interface-range*

Syntax Description

macro-name	Name of the interface-range macro; up to 32 characters.
interface-range	Interface range; for valid values for interface ranges, see "Usage Guidelines."

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The macro name is a 32-character maximum character string.

A macro can contain up to five ranges.

All interfaces in a range must be the same type; that is, all Gigabit Ethernet ports, all TenGigabit Ethernet ports, all EtherChannel ports, or all VLANs, but you can combine multiple interface types in a macro.

When entering the *interface-range*, use this format:

- *type* {*first-interface*} - {*last-interface*}
- You must add a space between the first interface number and the hyphen when entering an *interface-range*. For example, **gigabitethernet 0/1 - 2** is a valid range; **gigabitethernet 0/1-2** is not a valid range

Valid values for *type* and *interface*:

- **vlan** *vlan-id*, where *vlan-id* is from 1 to 4094

  VLAN interfaces must have been configured with the **interface vlan** command (the **show running-config** privileged EXEC command displays the configured VLAN interfaces). VLAN interfaces not displayed by the **show running-config** command cannot be used in *interface-ranges.*
- **port-channel** *port-channel-number*, where *port-channel-number* is from 1 to 48
- **gigabitethernet** *module*/{*first port*} - {*last port*}
- **tengigabitethernet** *module*/{*first port*} - {*last port*}

For physical interfaces:

- module is always 0.
- the range is *type* **0**/*number* - *number* (for example, **gigabitethernet 0/1 - 2**).

When you define a range, you must enter a space before the hyphen (-), for example:

gigabitethernet0/1 - 2

You can also enter multiple ranges. When you define multiple ranges, you must enter a space after the first entry before the comma (,). The space after the comma is optional, for example:

gigabitethernet0/3, tengigabitethernet0/1 - 2

gigabitethernet0/3 -4, tengigabitethernet0/1 - 2

Examples

This example shows how to create a multiple-interface macro:

```
Switch(config)# define interface-range macro1 fastethernet0/1 - 2, gigabitethernet0/1 - 2
```

Related Commands

Command	Description
interface range	Executes a command on multiple ports at the same time.
show running-config	Displays the operating configuration.

delete

To delete a file or directory on the flash memory device, use the **delete** command in privileged EXEC mode.

delete [**/force**] [**/recursive**] {**flash** | **nvram**}

Syntax Description

/force	(Optional) Suppresses the prompt that confirms the deletion.
/recursive	(Optional) Deletes the named directory and all subdirectories and the files contained in it.
flash	Deletes the flash directory.
nvram	Deletes NVRAM.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If you use the **/force** keyword, you are prompted once at the beginning of the deletion process to confirm the deletion.

If you use the **/recursive** keyword without the **/force** keyword, you are prompted to confirm the deletion of every file.

The prompting behavior depends on the setting of the **file prompt** global configuration command. By default, the switch prompts for confirmation on destructive file operations. For more information about this command, see the *Cisco IOS Command Reference for Release 12.2*.

Examples

This example shows how to remove the directory that contains the old software image after a successful download of a new image:

```
Switch# delete /force /recursive flash:/old-image
```

You can verify that the directory was removed by entering the **dir** *filesystem***:** privileged EXEC command.

Related Commands

Command	Description
archive download-sw	Downloads a new image to the switch and overwrites or keeps the existing image.

deny (MAC access-list configuration)

To prevent non-IP traffic from being forwarded if the conditions are matched, use the **deny** command in MAC access-list configuration mode. To remove a deny condition from the named MAC access list, use the **no** form of this command.

deny {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **cos** *cos* | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* |**mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**]

no deny {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **cos** *cos* | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**]

Syntax Description

any	Keyword to specify to deny any source or destination MAC address.
host *src MAC-addr* | *src-MAC-addr mask*	Defines a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied.
host *dst-MAC-addr* | *dst-MAC-addr mask*	Defines a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied.
type mask	(Optional) Uses the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. • The *type* is 0 to 65535, specified in hexadecimal. • The *mask* is a mask of *don't care* bits applied to the Ethertype before testing for a match.
aarp	(Optional) Selects Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber	(Optional) Selects EtherType DEC-Amber.
cos *cos*	(Optional) Selects a class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message reminds the user if the **cos** option is configured.
dec-spanning	(Optional) Selects EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv	(Optional) Selects EtherType DECnet Phase IV protocol.
diagnostic	(Optional) Selects EtherType DEC-Diagnostic.
dsm	(Optional) Selects EtherType DEC-DSM.
etype-6000	(Optional) Selects EtherType 0x6000.
etype-8042	(Optional) Selects EtherType 0x8042**.**
lat	(Optional) Selects EtherType DEC-LAT.
lavc-sca	(Optional) Selects EtherType DEC-LAVC-SCA.

lsap *lsap-number mask*	(Optional) Uses the LSAP number (0 to 65535) of a packet with IEEE 802.2 encapsulation to identify the protocol of the packet. *mask* is a mask of *don't care* bits applied to the LSAP number before testing for a match.
mop-console	(Optional) Selects EtherType DEC-MOP Remote Console.
mop-dump	(Optional) Selects EtherType DEC-MOP Dump.
msdos	(Optional) Selects EtherType DEC-MSDOS.
mumps	(Optional) Selects EtherType DEC-MUMPS.
netbios	(Optional) Selects EtherType DEC- Network Basic Input/Output System (NETBIOS).
vines-echo	(Optional) Selects EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	(Optional) Selects EtherType VINES IP.
xns-idp	(Optional) Selects EtherType Xerox Network Systems (XNS) protocol suite (0 to 65535), an arbitrary Ethertype in decimal, hexadecimal, or octal.

Note Though visible in the command-line help strings, **appletalk** is not supported as a matching condition.

To filter IPX traffic, you use the *type mask* or **lsap** *lsap mask* keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in Table 2-1.

Table 2-1 IPX Filtering Criteria

IPX Encapsulation Type		
Cisco IOS Name	**Novel Name**	**Filter Criterion**
arpa	Ethernet II	Ethertype 0x8137
snap	Ethernet-snap	Ethertype 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

Defaults

This command has no defaults. However; the default action for a MAC-named ACL is to deny.

Command Modes

MAC-access list configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You enter MAC-access list configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **host** keyword, you must enter an address mask.

When an access control entry (ACE) is added to an access control list, an implied **deny**-**any**-**any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

Note For more information about named MAC extended access lists, see the software configuration guide for this release.

You can verify your settings by entering the **show access-lists** privileged EXEC command.

Examples

This example shows how to define the named MAC extended access list to deny NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is denied.

```
Switch(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

This example shows how to remove the deny condition from the named MAC extended access list:

```
Switch(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

This example denies all packets with Ethertype 0x4321:

```
Switch(config-ext-macl)# deny any any 0x4321 0
```

Related Commands

Command	Description
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.
permit (MAC access-list configuration)	Permits non-IP traffic to be forwarded if conditions are matched.
show access-lists	Displays access control lists configured on a switch.

diagnostic schedule test

To configure the diagnostic test schedule, use the **diagnostic schedule test** command in global configuration mode. to remove the schedule, use the **no** form of this command.

diagnostic schedule test {*name* | *test-id* | *test-id-range* | **all** | **basic**} {**daily** *hh*:*mm* | **on** *mm dd yyyy hh*:*mm* | **weekly** *day-of-week hh*:*mm*}

no diagnostic schedule test {*name* | *test-id* | *test-id-range* | **all** | **basic**} {**daily** *hh*:*mm* | **on** *mm dd yyyy hh*:*mm* | **weekly** *day-of-week hh*:*mm*}

Syntax Description

name	Specifies the name of the test. To display the test names in the test-ID list, enter the **show diagnostic content** privileged EXEC command.
test-id	Specifies the ID number of the test. The range is from 1 to 6. To display the test numbers in the test-ID list, enter the **show diagnostic content** privileged EXEC command.
test-id-range	Specifies more than one test with the range of test ID numbers. Enter the range as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6). To display the test numbers in the test-ID list, enter the **show diagnostic content** privileged EXEC command.
all	Specifies all of the diagnostic tests.
basic	Specifies the basic on-demand diagnostic tests.
daily *hh*:*mm*	Specifies the daily scheduling of the diagnostic tests. *hh*:*mm*—Enter the time as a 2-digit number (for a 24-hour clock) for hours:minutes; the colon (:) is required, such as 12:30.
on *mm dd yyyy hh*:*mm*	Specifies the scheduling of the diagnostic tests on a specific day and time. For *mm dd yyyy*: • *mm*—Spell out the month, such as January, February, and so on, with upper-case or lower-case characters. • *dd*—Enter the day as a 2-digit number, such as 03 or 16. • *yyyy*—Enter the year as a 4-digit number, such as 2008.
weekly *day-of-week hh*:*mm*	Specifies the weekly scheduling of the diagnostic tests. *day-of-week*—Spell out the day of the week, such as Monday, Tuesday, and so on, with upper-case or lower-case characters.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to schedule diagnostic testing for a specific day and time:

```
Switch(config)# diagnostic schedule test 1,2,4-6 on november 3 2006 23:10
```

This example shows how to schedule diagnostic testing to occur weekly at a specific time:

```
Switch(config)# diagnostic schedule test TestPortAsicMem weekly friday 09:23
```

Related Commands

Command	Description
show diagnostic	Displays online diagnostic test results.

diagnostic start test

To run an online diagnostic test, use the **diagnostic start test** command in privileged EXEC mode.

diagnostic start test {*name* | *test-id* | *test-id-range* | **all** | **basic**}

Syntax Description

name	Specifies the name of the test. To display the test names in the test-ID list, enter the **show diagnostic content** privileged EXEC command.
test-id	Specifies the ID number of the test. The range is from 1 to 6. To display the test numbers in the test-ID list, enter the **show diagnostic content** privileged EXEC command.
test-id-range	Specifies more than one test with the range of test ID numbers. Enter the range as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6). To display the test numbers in the test-ID list, enter the **show diagnostic content** privileged EXEC command.
all	Specifies all the diagnostic tests.
basic	Specifies the basic on-demand diagnostic tests.

Defaults

This command has no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

After you start the tests by using the **diagnostic start** command, you cannot stop the testing process.

The switch supports these tests:

```
ID   Test Name [On-Demand Test Attributes]
---  -----------------------------------------
1    TestPortAsicMem [B*D*R**]
2    TestPortAsicCam [B*D*R**]
3    TestPortAsicLoopback [B*D*R**]
4    TestPortLoopback [B*D*R**]
5    TestFpga [B*D*R**]
---  -----------------------------------------
```

To identify a test name, use the **show diagnostic content** privileged EXEC command to display the test ID list. To specify test 3 by using the test name, enter the **diagnostic start switch** *number* **test TestPortAsicCam** privileged EXEC command.

To specify more than one test, use the *test-id-range* parameter, and enter integers separated by a comma and a hyphen. For example, to specify tests 2, 3, and 4, enter the **diagnostic start test 2-4** command. To specify tests 1, 3, 4, 5, and 6, enter the **diagnostic start test 1,3-6** command.

Examples

This example shows how to start diagnostic test 1:

```
Switch# diagnostic start test 1
Switch#
06:27:50: %DIAG-6-TEST_RUNNING: Running TestPortAsicMem {ID=1} ...
06:27:51: %DIAG-6-TEST_OK: TestPortAsicSMem {ID=1} has completed
successfully
```

This example shows how to start diagnostic test 3. Running this test disrupts the normal system operation and then reloads the switch.

```
Switch# diagnostic start test 3
Running test(s) 3 will cause the switch under test to reload after completion of
the test list.
Running test(s) 2 may disrupt normal system operation
Do you want to continue? [no]: y
Switch#
00:00:25: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
00:00:29: %SYS-5-CONFIG_I: Configured from memory by console
00:00:30: %DIAG-6-TEST_RUNNING : Running TestPortAsicLoopback{ID=2} ...
00:00:30: %DIAG-6-TEST_OK: TestPortAsicLoopback{ID=2} has completed successfully
```

Related Commands

Command	Description
show diagnostic	Displays online diagnostic test results.

distribution

To configure statistics distributions for an IP Service Level Agreements (SLAs) Metro-Ethernet 3.0 (ITU-T Y.1731) operation, use the **distribution** command in IP SLA Y.1731 delay configuration mode. To return to the default value, use the no form of the command.

distribution {**delay** | **delay-variation**} {**one-way** | **two-way**} *number-of-bins boundary*[,...,*boundary*]

no distribution {delay | delay-variation} {one-way | two-way}

Syntax Description

delay	Specifies that the performance measurement type is delay. This is the default value, along with delay variation.
delay-variation	Specifies that the performance measurement type is delay variation. This is the default value, along with delay.
one-way	Specifies one-way measurement values. This is the default for a dual-ended operation.
two-way	Specifies two-way measurement values. This is the default for a single-ended operation.
number-of-bins	Number of bins kept during an aggregate interval. Range is from 1 to 10. Default is 10.
boundary [,...,boundary]	List of upper boundaries for bins in microseconds. Minimum number of boundaries required is one. Maximum allowed value for the uppermost boundary is -1 microsecond. Multiple values must be separated by a comma (,). Default is 5000,10000,15000,20000,25000,30000,35000,40000,45000, -1.

Defaults

The default for distribution is 10 bins with upper boundaries of 5000, 10000,15000,20000,25000,30000,35000,40000,45000,-1, for both delay and delay-variation performance measurements.

Command Modes

IP SLA Y.1731 delay configuration (config-sla-y1731-delay)

Command History

Release	Modification
15.2(4)S1	This command was introduced.

Usage Guidelines

Use this command change the type of performance measurements to be calculated and the number and range of distribution bins from the defaults (10 bins with upper boundaries of 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1, for both delay and delay-variation performance measurements) to the specified values.

Configure this command on the Maintenance End Point (MEP) that performs the performance measurement calculation. For single-ended operations, calculations are performed at the sender MEP. For dual-ended operations, calculations are performed at the receiver MEP on the responder.

Statistics distributions are defined by number and range of bins per interval.

A bin is a counter that counts the number of measurements initiated and completed during a specified length of time for each operation. The results of performance measurements falling within a specified range are stored in each bin. When the number of distributions reaches the number and range specified, no further distribution-based information is stored.

The lower bound value for the first upper boundary is always 0 microseconds, such as 0 to 5000 microseconds for the default first upper boundary.

The maximum allowed value for the uppermost boundary is -1 microsecond.

An aggregate interval is the length of time during which the performance measurements are conducted and the results stored. You can configure the interval by using the aggregate interval command.

To avoid significant impact on router memory, careful consideration should be used when configuring distribution.

Examples

The following example shows how to configure the sender MEP to calculate two-way, delay-variation performance measurements for a single-ended IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) operation, and store the statistics in five bins:

```
Switch(config-term)# diagnostic start test 1
Switch(config-term)# ip sla 10
Switch(config-ip-sla)# ethernet y1731 delay dmm domain xxx evc yyy mpid 101 cos 3 source
mpid 100
Switch(config-sla-y1731-delay)# distribution delay-variation two-way 5
5000,10000,15000,20000-1
Switch(config-sla-y1731-delay)#This example shows how to start diagnostic test 3. Running
this test disrupts the normal system operation and then reloads the switch.
```

Related Commands

Command	Description
aggregate interval	Configures the aggregate interval.
history interval	Sets the number of statistics distributions kept during the lifetime of an IP SLAs Metro Ethernet 3.0 (ITU-T Y.1731) operation.

duplex

To specify the duplex mode of operation for a port, use the **duplex** command in interface configuration mode. To return the port to its default value, use the **no** form of this command.

duplex {**auto** | **full** | **half**}

no duplex

Note This command is not available on 10 Gigabit Ethernet ports.

Syntax Description

auto	Enables automatic duplex configuration; port automatically detects whether it should run in full- or half-duplex mode, depending on the attached device mode.
full	Enables full-duplex mode.
half	Enables half-duplex mode (only for interfaces operating at 10 Mbps or 100 Mbps). You cannot configure half-duplex mode for interfaces operating at 1000 Mbps or 10,000 Mbps.

Defaults

The default is **auto** for Fast Ethernet and Gigabit Ethernet ports and for 1000BASE-T small form-factor pluggable (SFP) modules.

The default is **half** for 100BASE-FX MMF SFP modules.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

This command is visible for an SPP module only when a 1000BASE-T SFP module or a 100BASE-FX MMF SFP module is in the SFP module slot. All other SFP modules operate only in full-duplex mode.

- When a 1000BASE-T SFP module is in the SFP module slot, you can configure duplex mode to **auto** or **full**.
- When a 100BASE-FX MMF SFP module is in the SFP module slot, you can configure duplex mode to **half** or **full**. Although the **auto** keyword is available, it puts the interface in half-duplex mode (the default) because the 100BASE-FX MMF SFP module does not support autonegotiation.

Certain ports can be configured to be either full duplex or half duplex. Applicability of this command depends on the device to which the switch is attached.

For Gigabit Ethernet ports, setting the port to **auto** has the same effect as specifying **full** if the attached device does not autonegotiate the duplex parameter.

Note Half-duplex mode is supported on Gigabit Ethernet interfaces if duplex mode is **auto** and the connected device is operating at half duplex. However, you cannot configure these interfaces to operate in half-duplex mode.

If both ends of the line support autonegotiation, we highly recommend using the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces; do use the **auto** setting on the supported side.

If the speed is set to **auto**, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.

You can configure the duplex setting when the speed is set to **auto**.

Caution Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

Note For guidelines on setting the switch speed and duplex parameters, see the software configuration guide for this release.

You can verify your setting by entering the **show interfaces** privileged EXEC command.

Examples

This example shows how to configure an interface for full duplex operation:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# duplex full
```

Related Commands

Command	Description
show interfaces	Displays the interface settings on the switch.
speed	Sets the speed on a 10/100 or 10/100/1000 Mbps interface.

errdisable detect cause

To enable error-disabled detection for a specific cause or all causes, use the **errdisable detect cause** command in global configuration mode. To disable the error-disabled detection feature, use the **no** form of this command.

errdisable detect cause {**all** | **bpduguard** | **gbic-invalid** | **link-flap** | **loopback** | **pagp-flap** | **ppoe-ia-rate-limit** | **security-violation** | **sfp-config-mismatch**}

no errdisable detect cause {**all** | **bpduguard** | **gbic-invalid** | **link-flap** | **loopback** | **pagp-flap** | **ppoe-ia-rate-limit** | **security-violation** | **sfp-config-mismatch**}

Note Although visible in the command-line help, the **arp-inspection** and **dhcp rate-limit** keywords are not supported.

Syntax Description

all	Enables error detection for all error-disable causes.
gbic-invalid	Enables error detection for an invalid Gigabit Interface Converter (GBIC) module. **Note** This error refers to an invalid small form-factor pluggable (SFP) module.
link-flap	Enables error detection for link-state flapping.
loopback	Enables error detection for detected loopbacks.
pagp-flap	Enables error detection for the Port Aggregation Protocol (PAgP) flap error-disabled cause.
ppoe-ia-rate-limit	Enables error detection for Point-to-Point Protocol over Ethernet (ppoe) rate limit.
security-violation	Enables error detection for security violations.
sfp-config-mismatch	Enables error detection on SFP configuration mismatch.

Defaults

Detection is enabled for all causes. All causes, except for per-VLAN error disabling**,** are configured to shut down the entire port.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

A cause (**all**, **link-flap**, and so forth) is the reason why the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in an error-disabled state, an operational state that is similar to a link-down state.

When a port is error-disabled, it is effectively shut down, and no traffic is sent or received on the port. For the BPDU guard and port-security features, you can configure the switch to shut down just the offending VLAN on the port when a violation occurs, instead of shutting down the entire port.

If you set a recovery mechanism for the cause by entering the **errdisable recovery** global configuration command for the cause, the interface is brought out of the error-disabled state and allowed to retry the operation when all causes have timed out. If you do not set a recovery mechanism, you must enter the **shutdown** and then the **no shutdown** commands to manually recover an interface from the error-disabled state.

You can verify your setting by entering the **show errdisable detect** privileged EXEC command.

Examples

This example shows how to enable error-disabled detection for the link-flap error-disabled cause:

```
Switch(config)# errdisable detect cause link-flap
```

Related Commands

Command	Description
show errdisable detect	Displays errdisable detection information.
show interfaces status err-disabled	Displays interface status or a list of interfaces in the error-disabled state.

errdisable recovery

To configure the recover mechanism variables, use the **errdisable recovery** command in global configuration mode. To return to the default setting, use the **no** form of this command.

errdisable recovery {**cause** {**all** | **bpduguard** | **channel-misconfig** | **gbic-invalid** | **link-flap** | **loopback** | **mac-limit** | **pagp-flap** | **oam-remote failure** | **port-mode failure** | **ppoe-ia-rate-limit** | **storm-control** | **unicast-flood** | | **udld**} | {**interval** *interval*}

no errdisable recovery {**cause** {**all** | **bpduguard** | **channel-misconfig** | **gbic-invalid** | **link-flap** | **loopback** | **mac-limit** | **pagp-flap** | **oam-remote failure** | **port-mode failure** | **ppoe-ia-rate-limit** | **storm-control** | **unicast-flood** | | **udld**} | {**interval** *interval*}

Note Although visible in the command-line help, the **dhcp-rate-limit** and **psecure-violation** keywords are not supported.

Syntax Description

cause	Enables the error-disabled mechanism to recover from a specific cause.
all	Enables the timer to recover from all error-disabled causes.
bpduguard	Enables the timer to recover from the bridge protocol data unit (BPDU) guard error-disabled state.
channel-misconfig	Enables the timer to recover from the EtherChannel misconfiguration error-disabled state.
gbic-invalid	Enables the timer to recover from an invalid Gigabit Interface Converter (GBIC) module error-disabled state. **Note** This error refers to an invalid small form-factor pluggable (SFP) error-disabled state.
link-flap	Enables the timer to recover from the link-flap error-disabled state.
loopback	Enables the timer to recover from a loopback error-disabled state.
mac-limit	Enables the timer to recover from the MAC limit disable state.
oam-remote failure	Enables the timer to recover from an Ethernet Operations, Administration, and Maintenance (OAM) detected remote failure.
pagp-flap	Enables the timer to recover from the Port Aggregation Protocol (PAgP)-flap error-disabled state.
port-mode failure	Enables the timer to recover from port mode change
ppoe-ia-rate-limit	Enables the timer to recover from Point-to-Point Protocol over Ethernet (PPPoE) IA rate-limit.
udld	Enables the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state.
unicast-flood	Enables the timer to recover from the unicast flood disable state.

interval *interval*	Specifies the time to recover from the specified error-disabled state. The range is 30 to 86400 seconds. The same interval is applied to all causes. The default interval is 300 seconds. **Note** The error-disabled recovery timer is initialized at a random differential from the configured interval value. The difference between the actual timeout value and the configured value can be up to 15 percent of the configured interval.

Note Although visible in the command-line interface help, the **arp-inspection**, **security-violation**, and **vmps** keywords are not supported.

Defaults

Recovery is disabled for all causes.

The default recovery interval is 300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

A cause (**all**, **bpduguard** and so forth) is defined as the reason that the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in error-disabled state, an operational state similar to link-down state. If you do not enable errdisable recovery for the cause, the interface stays in error-disabled state until you enter a **shutdown** and **no shutdown** interface configuration command. If you enable the recovery for a cause, the interface is brought out of the error-disabled state and allowed to retry the operation again when all the causes have timed out.

Otherwise, you must enter the **shutdown** then **no shutdown** commands to manually recover an interface from the error-disabled state

You can verify your settings by entering the **show errdisable recovery** privileged EXEC command.

Examples

This example shows how to enable the recovery timer for the BPDU guard error-disabled cause:

```
Switch(config)# errdisable recovery cause bpduguard
```

This example shows how to set the timer to 500 seconds:

```
Switch(config)# errdisable recovery interval 500
```

Related Commands

Command	Description
show errdisable recovery	Displays errdisable recovery timer information.
show interfaces status err-disabled	Displays interface status or a list of interfaces in error-disabled state.

ethernet evc

To define an Ethernet virtual connection (EVC) and to enter EVC configuration mode, use the **ethernet evc** command in global configuration mode.To delete the EVC, use the **no** form of this command.

ethernet evc *evc-id*

no ethernet evc *evc-id*

Syntax Description

evc-id	The EVC identifier. This can be a string of from 1 to 100 characters.

Defaults

No EVCs are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

After you enter the **ethernet evc** *evc-id* command, the switch enters EVC configuration mode, and these configuration commands are available:

- **default**: sets the EVC to its default states.
- **exit**: exits EVC configuration mode and returns to global configuration mode.
- **no**: negates a command or returns a command to its default setting.
- **oam protocol cfm svlan**: configures the Ethernet operation, administration, and maintenance (OAM) protocol as IEEE 802.1ag Connectivity Fault Management (CFM) and sets parameters. See the **oam protocol cfm svlan** command.
- **uni count**: configures a UNI count for the EVC. See the **uni count** command.

Examples

This example shows how to define an EVC and to enter EVC configuration mode:

```
Switch(config)# ethernet evc test1
Switch(config-evc)#
```

Related Commands

Command	Description
service instance *id* **ethernet** *evc-id*	Configures an Ethernet service instance and attaches an EVC to it.
show ethernet service evc	Displays information about configured EVCs.

ethernet lmi

To configure enable Ethernet Local Management Interface (E-LMI) and to configure the switch as a customer-edge (CE) device, use the **ethernet lmi** command in global configuration mode. To disable E-LMI globally or to disable E-LMI CE, use the **no** form of this command.

ethernet lmi {**ce** | **global**}

no ethernet lmi {**ce** | **global**}

Syntax Description

ce	Enables the switch as an E-LMI CE device. **Note** The switch can only be an E-LMI CE device.
global	Enables E-LMI globally on the switch.

Defaults

Ethernet LMI is disabled. When enabled with the global keyword, by default the switch is a PR device.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use **ethernet lmi global** command to enable E-LMI globally. Use **ethernet lmi ce** command to enable the switch as E-LMI CE device.

Ethernet LMI is disabled by default on an interface and must be explicitly enabled by entering the **ethernet lmi interface** interface configuration command. The **ethernet lmi global** command enables Ethernet LMI on all interfaces for an entire device. The benefit of this command is that you can enable Ethernet LMI on all interfaces with one command instead of enabling Ethernet LMI separately on each interface. To enable the interface in CE mode, you must also enter the **ethernet lmi ce** global configuration command.

To disable Ethernet LMI on a specific interface after you have entered the **ethernet lmi global** command, enter the **no ethernet lmi interface** interface configuration command.

The sequence in which you enter the **ethernet lmi interface** interface configuration and **ethernet lmi global** global configuration commands is important. The latest command entered overrides the prior command entered.

Note For information about the **ethernet lmi** interface configuration command, see the *Cisco IOS Carrier Ethernet Command Reference* at this URL:
http://www.cisco.com/en/US/docs/ios/cether/command/reference/ce_book.html

To enable the switch as an Ethernet LMI CE device, you must enter both the **ethernet lmi global** and **ethernet lmi ce** commands. By default Ethernet LMI is disabled.

When the switch is configured as an Ethernet LMI CE device, these interface configuration commands and keywords are visible, but not supported:

- **service instance**
- **ethernet uni**
- **ethernet lmi t392**

Examples

This example shows how to configure the switch as an Ethernet LMI CE device:

```
Switch(config)# ethernet lmi global
Switch(config)# ethernet lmi ce
```

Related Commands

Command	Description
ethernet lmi interface configuration command	Enables Ethernet LMI for a user-network interface.

ethernet oam remote-failure

To configure Ethernet operations, maintenance, and administration (EOM) remote failure indication, use the **ethernet oam remote-failure** command in interface configuration or configuration template mode. To remove the configuration, use the **no** form of this command.

ethernet oam remote-failure {**critical-event** | **dying-gasp** | **link-fault**} **action** **error-disable-interface**

no ethernet oam remote-failure {**critical-event** | **dying-gasp** | **link-fault**} **action**

Syntax Description

critical-event	Configures the switch to put an interface in error-disabled mode when an unspecified critical event has occurred.
dying-gasp	Configures the switch to put an interface in error-disabled mode when an unrecoverable condition has occurred.
link-fault	Configures the switch to put an interface in error-disabled mode when the receiver detects a loss of power.

Defaults

Configuration template

Interface configuration

Command Modes

Ethernet service configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can apply this command to an Ethernet OAM template and to an interface. The interface configuration takes precedence over template configuration. To enter OAM template configuration mode, use the **template** *template-name* global configuration command.

The switch does not generate Link Fault or Critical Event OAM PDUs. However, if these PDUs are received from a link partner, they are processed. The switch supports generating and receiving Dying Gasp OAM PDUs when Ethernet OAM is disabled, the interface is shut down, the interface enters the error-disabled state, or the switch is reloading. The switch can also generate and receive Dying Gasp PDUs based on loss of power. The PDU includes a reason code to indicate why it was sent.

You can configure an error-disable action to occur if the remote link goes down, if the remote device is disabled, or if the remote device disables Ethernet OAM on the interface.

For complete command and configuration for the Ethernet OAM protocol, see the *Cisco IOS Carrier Ethernet Configuration Guide* at this URL:
http://www.cisco.com/en/US/docs/ios/cether/configuration/guide/12_2sr/ce_12_2sr_book.html

ethernet uni id

To create an Ethernet user-network interface (UNI) ID, use the **ethernet uni** command in interface configuration mode.To remove the UNI ID, use the **no** form of this command.

ethernet uni id *name*

no ethernet uni id

Syntax Description

name	Identifies an Ethernet UNI ID. The name should be unique for all UNIs that are part of a given service instance and can be up to 64 characters in length.

Defaults

No UNI IDs are created.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When you configure a UNI ID on a port, that ID is used as the default name for all maintenance end points (MEPs) configured on the port.

You must enter the **ethernet uni id** *name* command on all ports that are directly connected to customer-edge (CE) devices. If the specified ID is not unique on the device, an error message appears.

Examples

This example shows how to identify a unique UNI:

```
Switch(config-if)# ethernet uni id test2
```

Related Commands

Command	Description
show interfaces	Displays information about Ethernet service instances on an interface, including service type.

ethernet y1731 delay

To configure a sender Maintenance End Point (MEP) for an IP Service Level Agreements (SLAs) Metro Ethernet 3.0 (UIT-T Y.1731) delay or delay variation operation, use the ethernet y1731delay command in IP SLA configuration mode.

ethernet y1731 delay DMM domain *domain* {{**vlan** | **evc**} *value*}{**mpid** | **mac-address**} *value* **cos** *value* **source** {**mpid** | **mac-address**} *value*

Syntax Description

DMM	Specifies that the frames sent are Delay Measurement Message (DMM) synthetic frames.
domain *domain*	Specifies name of the Ethernet Connectivity Fault Management (CFM) maintenance domain.
vlan	Specifies the VLAN identification number. The range is from 1 to 4096.
evc	Specifies the Ethernet Virtual Circuit (EVC) identification name.
mpid	Specifies the maintenance endpoint identification numbers of the MEP at the destination. The range is from 1 to 8191.
mac-address	Specifies the MAC address of the MEP at the destination.
cos	Specifies, for this MEP, which class of service (CoS) that will be sent in the Ethernet connectivity fault management (CFM) message. The range is from 0 to 7.
source mpid	List of maintenance endpoint identification numbers of the MEP being configured. The range is from 1 to 8191.
source mac-address	MAC address of the MEP being configured.

Defaults

A sender MEP is not configured for theiP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) operation.

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

This command begins configuring a sender MEP for an Ethernet Frame Delay (ETH-DM: FD) operation and enters IP SLA Y.1731 delay configuration mode.

The **DMM** keyword for this command is not case sensitive. The keyword in online help contains uppercase letters to enhance readability only.

To change the operation type of an existing IP SLAs operation, you must first use the **no ip sla** command to delete the IP SLAs operation and then reconfigure the iperation with the new operation type.

Examples

This example shows how configure an MEP for a two way frame delay or delay variation operation.

```
Switch# enable
Switch# configure terminal
Switch(config)# ip sla 1
Switch(config-ip-sla)# ethernet y1731 delay DMM domain ifm_400 evc e1 mpid 401 cos 4
source mpid 1
Switch(config-sla-y1731-delay)#
```

Related Commands

Command	Description
no ip sla	Deletes an existing configuration for a Cisco IP SLAs operation

ethernet y1731 loss

To configure a sender Maintenance End Point (MEP) for an IP Service Level Agreements (SLAs) Metro Ethernet 3.0 (UIT-T Y.1731) frame loss operation, use the **ethernet y1731 loss** command in IP SLA configuration mode.

ethernet y1731 loss SLM [**burst**] **domain** *domain* {{**vlan** | **evc**} *value*}{**mpid** | **mac-address**} *value* **cos** *value* **source** {**mpid** | **mac-address**} *value*

Syntax Description

SLM	Specifies that the frames sent are Synthetic Loss Message (DMM) synthetic frames.
burst	Specifies that frames will be sent in a burst.
domain *domain*	Specifies name of the Ethernet Connectivity Fault Management (CFM) maintenance domain.
vlan	Specifies the VLAN identification number. The range is from 1 to 4096.
evc	Specifies the Ethernet Virtual Circuit (EVC) identification name.
mpid	Specifies the maintenance endpoint identification numbers of the MEP at the destination. The range is from 1 to 8191.
mac-address	Specifies the MAC address of the MEP at the destination.
cos	Specifies, for this MEP, which class of service (CoS) that will be sent in the Ethernet connectivity fault management (CFM) message. The range is from 0 to 7.
source mpid	List of maintenance endpoint identification numbers of the MEP being configured. The range is from 1 to 8191.
source mac-address	MAC address of the MEP being configured.

Defaults

A sender MEP is not configured for the IP SLAs Metro-Ethernet 3.0 (ITU-T Y.1731) operation.

Command Modes

IP SLA configuration (config-ip-sla)

Command History

Release	Modification
15.2(4)S	This command was introduced.

Usage Guidelines

This command begins configuring a sender MEP for an Ethernet Synthetic Loss Measurement (ETH-SLM) and enters IP SLA Y.1731 loss configuration mode.

The **SLM** keyword for this command is not case sensitive. The keyword in online help contains uppercase letters to enhance readability only.

You must configure CoS-level monitoring, use the **monitor loss counter** [**priority** *cos range*] command under the EVC CFM sub-config mode for those interfaces that require loss monitoring.

To change the operation type of an existing IP SLAs operation, you must first use the **no ip sla** command to delete the IP SLAs operation and then reconfigure the iperation with the new operation type.

Examples

This example shows how configure an MEP for synthetic loss measurement.

```
Switch# enable
Switch# configure terminal
Switch(config)# ip sla 1
Switch(config-ip-sla)# ethernet y1731 loss SLM domain r3 vlan 10 mpid 3 cos 1 source mpid
1
Switch(config-sla-y1731-loss)#
```

Related Commands

Command	Description
monitor loss counters	Enables COS-level monitoring.
no ip sla	Deletes an existing configuration for an IP SLAs operation.

exceed-action

To set actions for a policy-map class for packets that conform to the peak information rate (PIR) but not the committed information rate (CIR), use the **exceed-action** command in policy-map class police configuration mode. To cancel the action or to return to the default action, use the **no** form of this command.

exceed-action {**drop** | **set-cos-transmit** *new cos-value* | **set-discard-class-transmit** *new discard-value* | **set-dscp-transmit** *new dscp-value* | **set-mpls-exp-imposition-transmit** *new-imposition-exp-value* | **set-mpls-exp-topmost transmit** *new-topmost-exp-value* | **set-prec-transmit value** *new prec-value* | **set-qos-transmit value** *new qos-value*| **transmit**}

no exceed-action {**drop** | **set-cos-transmit** *new cos-value* | **set-discard-class-transmit** *new discard-value* | **set-dscp-transmit** *new dscp-value* | **set-mpls-exp-imposition-transmit** *new-imposition-exp-value* | **set-mpls-exp-topmost transmit** *new-topmost-exp-value* | **set-prec-transmit value** *new prec-value* | **set-qos-transmit value** *new qos-value*| **transmit**}

Syntax Description

drop	Drops the packet.
set-cos-transmit *new-cos-value*	Sets a new class of service (CoS) value for the packet and send the packet. The range for the new CoS value is 0 to 7.
set-discard-class-transmit *new discard-value*	Sets a new discard-class value for the packet and send the packet. The range for the value is 0 to 7.
set-dscp-transmit *new-dscp-value*	Sets a new Differentiated Services Code Point (DSCP) value for the packet and send the packet. The range for the new DCSP value is 0 to 63.
set-mpls-exp-imposition transmit *new-imposition-exp-value*	Sets an MPLS label using the new MPLS EXP value at tag imposition, and send the packet. The range is 0 to 7.
set-mpls-exp-topmost transmit *new-topmost-exp-value*	Sets an MPLS label using the new MPLS EXP value for the topmost (outer) MPLS label, and send the packet. The range is 0 to 7.
set-prec-transmit *new-precedence-value*	Sets a new IP precedence value for the packet and send the packet. The range for the new IP precedence value is 0 to 7.
set-qos-transmit *qos-group-value*	Sets a new quality of service (QoS) group value for the packet and send the packet. The range for the new QoS value is 0 to 99.
transmit	Sends the packet unmodified.

Defaults

The default action is to drop the packet.

Command Modes

Policy-map class police configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You configure exceed actions for packets that conform to the peak information rate but not the committed information rate (CIR).

The switch also supports simultaneously marking multiple QoS parameters for the same class and configuring conform-action, exceed-action, and violate-action marking.

Access policy-map class police configuration mode by entering the **police** policy-map class command. See the **police** policy-map class configuration command for more information.

You can use this command to set one or more exceed actions for a traffic class.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how configure multiple actions in a policy map that sets a committed information rate of 5000000 bits per second (b/s) and a peak rate of 8000000 b/s:

```
Switch(config)# policy-map map1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police cir 5000000 pir 8000000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit 24
Switch(config-pmap-c-police)# violate-action drop
Switch(config-pmap-c-police)# end
```

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
conform-action	Defines the action to take on traffic that conforms to the CIR.
police	Defines a policer for classified traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays QoS policy maps.
violate-action	Defines the action to take on traffic with a rate greater than the conform rate plus the exceed burst.

flowcontrol

To set the receive flow-control state for an interface, use the **flowcontrol** command in interface configuration mode. When flow control **send** is operable and on for a device and it detects any congestion at its end, it notifies the link partner or the remote device of the congestion by sending a pause frame. When flow control **receive** is on for a device and it receives a pause frame, it stops sending any data packets. This prevents any loss of data packets during the congestion period.

To disable flow control, use the **receive off** keywords.

flowcontrol receive {**desired** | **off** | **on**}

Note The switch can only receive pause frames.

Syntax Description

receive	Sets whether the interface can receive flow-control packets from a remote device.
desired	Allows an interface to operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets.
off	Turns off the ability of an attached device to send flow-control packets to an interface.
on	Allows an interface to operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets.

Defaults

The default is **flowcontrol receive off**.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The switch does not support sending flow-control pause frames.

Note that the **on** and **desired** keywords have the same result.

When you use the **flowcontrol** command to set a port to control traffic rates during congestion, you are setting flow control on a port to one of these conditions:

- **receive on** or **desired**: The port cannot send out pause frames, but can operate with an attached device that is required to or is able to send pause frames; the port is able to receive pause frames.
- **receive off**: Flow control does not operate in either direction. In case of congestion, no indication is given to the link partner and no pause frames are sent or received by either device.

Table 2-2 shows the flow control results on local and remote ports for a combination of settings. The table assumes that **receive desired** has the same results as using the **receive on** keywords.

You can verify your settings by entering the **show interfaces** privileged EXEC command.

Table 2-2 Flow Control Settings and Local and Remote Port Flow Control Resolution

Flow Control Settings		Flow Control Resolution	
Local Device	**Remote Device**	**Local Device**	**Remote Device**
send off/receive on	**send on/receive on**	Receives only	Sends and receives
	send on/receive off	Receives only	Sends only
	send desired/receive on	Receives only	Sends and receives
	send desired/receive off	Receives only	Sends only
	send off/receive on	Receives only	Receives only
	send off/receive off	Does not send or receive	Does not send or receive
send off/receive off	**send on/receive on**	Does not send or receive	Does not send or receive
	send on/receive off	Does not send or receive	Does not send or receive
	send desired/receive on	Does not send or receive	Does not send or receive
	send desired/receive off	Does not send or receive	Does not send or receive
	send off/receive on	Does not send or receive	Does not send or receive
	send off/receive off	Does not send or receive	Does not send or receive

Examples

This example shows how to configure the local port to not support flow control by the remote port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# flowcontrol receive off
```

Related Commands

Command	Description
show interfaces	Displays the interface settings on the switch, including input and output flow control.

frame consecutive

To configure the number of consecutive measurements to be used to determine status for an IP Service Level Agreements (SLAs) Metro-Ethernet 3.0 (ITU-T Y.1731) frame loss operation, use the frame consecutive command in IP SLA Y.1731 loss configuration mode. To return to the default, use the no form of the command.

frame consecutive *number*

no frame consecutive *number*

Syntax Description

number	Number of consecutive measurements. The range is from 1 to 10. The default is 10.

Defaults

The default is ten consecutive frames.

Command Modes

IP SLA Y.1731 loss configuration (config-sla-y1731-loss)

Command History

Release	Modification
15.2(4)S1	This command was introduced.

Usage Guidelines

Availability is defined in terms of the ratio of frames lost to frames sent, or Frame Loss Ratio (FLR). Use this command to change the number of consecutive FLR measurements used to evaluate the status of an availability indicator from the default (10) to the specified number.

Examples

```
Switch(config-term)# ip sla 11
Switch(config-ip-sla)#ethernet y1731 loss LMM domain xxx vlan 12 mpid 34 cos 4 source mpid
23
Switch(config-sla-y1731-loss)# frame consecutive 5
Switch(config-sla-y1731-loss)#
```

frame interval

To configure the rate at which an IP Service Level Agreements (SLAs) Metro-Ethernet 3.0 (ITU-T Y.1731) operation sends synthetic frames, use the frame interval command in the IP SLA Y.1731 delay or IP SLA Y.1731 loss configuration mode. To return to the default, use the no form of the command.

frame interval *milliseconds*

no frame interval *milliseconds*

Syntax Description

milliseconds	Length of time in milliseconds (ms) between successive synthetic frames. The default is 1000. The valid values are: • 10--Frame interval is 10 ms • 100--Frame interval is 100 ms • 1000--Frame interval is 1000 ms (1 second) • 20--Frame interval is 20 ms • 25--Frame interval is 25 ms • 50--Frame interval is 50 ms

Defaults

The default for the frame interval is 1000 milliseconds.

Command Modes

IP SLA Y.1731 delay configuration (config-sla-y1731-delay)

IP SLA Y.1731 loss configuration (config-sla-y1731-loss)

Command History

Release	Modification
15.2(4)S1	This command was introduced.

Usage Guidelines

Use this command to change the gap between successive synthetic frames sent in an Ethernet delay, delay variation, or frame loss operation from the default (1000 ms) to the specified value.

Frames will be sent at a given frequency for the lifetime of the operation. For example, a delay operation with a frame interval of 1000 ms sends a frame once every second, for the lifetime of the operation.

Configure this command on the sender Maintenance End Point (MEP).

Examples

The following example shows how to configure the sender MEP for a single-ended IP SLAs Ethernet delay operation with a frame interval of 100 ms:

```
Switch(config-term)# ip sla 10
Switch(config-ip-sla)#ethernet y7131 delay dmm domain xxx evc yyy mpid 101 cos 3 source
mpid 100
Switch(config-sla-y1731-delay)# frame interval 100
Switch(config-sla-y1731-delay)# frame size 32
```

frequency (IP SLA)

To set the rate at which a specified IP Service Level Agreements (SLAs) operation repeats, use the frequency (IP SLA) command in the appropriate submode of IP SLA configuration or IP SLA monitor configuration mode. To return to the default value, use the no form of this command.

frequency *seconds*

no frequency

Syntax Description

seconds	Number of seconds between the IP SLAs operations. The default is 60.

Defaults

The default for frequency is 60 seconds.

Command Modes

IP SLA Y.1731 loss configuration (config-sla-y1731-loss)

Command History

Release	Modification
15.2(4)S1	This command was introduced.

Usage Guidelines

A single IP SLAs operation will repeat at a given frequency for the lifetime of the operation.

If an individual IP SLAs operation takes longer to execute than the specified frequency value, a statistics counter called "busy" is incremented rather than immediately repeating the operation.

For IP SLAs operations, the following configuration guideline is recommended:

(frequencyseconds) > (timeoutmilliseconds) > (thresholdmilliseconds)

Note We recommend that you do not set the frequency value to less than 60 seconds because the potential overhead from numerous active operations could significantly affect network performance.

Examples

The following example shows how to configure the sender MEP for a single-ended IP SLAs Ethernet delay operation with a frame interval of 100 ms:

```
Switch(config-term)# ip sla 10
Switch(config)# ip sla 2
Switch(config-ip-sla)# ethernet y1731 loss SLM burst domain r3 vlan 10 mpid 3 cos 2 source
mpid 1
Switch(config-sla-y1731-loss)# frequency 20
```

history interval

To set the number of statistics distributions kept during the lifetime of an IP Service Level Agreements (SLAs) Metro Ethernet 3.0 (ITU-T Y.1731) operation, use the history interval command in the IP SLA Y.1731 delay configuration or IP SLA Y.1731 loss configuration mode. To return to the default value, use the no form of this command.

history interval *intervals-stored*

no history interval

Syntax Description

intervals-stored	Number of statistics distributions. Range is 1 to 10. Default is 2.

Defaults

The default history interval is 2 distributions.

Command Modes

IP SLA Y.1731 loss configuration (config-sla-y1731-delay)

IP SLA Y.1731 loss configuration (config-sla-y1731-loss)

Command History

Release	Modification
15.2(4)S1	This command was introduced.

Usage Guidelines

Use this command to change the number of distribution statistics kept from the default (2) to the specified number.

Use the **distribution** command to configure the number and range of distribution bins to calculate delay and delay-variation performance measurements per interval.

Use the **aggregate interval** command to configure the length of time during which the performance measurements are conducted and the results stored for an Ethernet operation.

Examples

```
Switch(config-term)# ip sla 10
Switch(config-ip-sla)# ethernet y1731 delay dmm domain xxx evc yyy mpid 101 cos 3 source
mpid 100
Switch(config-sla-y1731-delay)# history interval 1
```

Related Commands

Command	Description
aggregate interval	Configures the aggregate interval.
distribution	Specifies measurement type and configures bins for statistics distributions kept for an Ethernet delay or delay variation operation.

hw-module module logging onboard

To enable on-board failure logging (OBFL), use the **hw-module module logging onboard** command in global configuration mode.To disable this feature, use the **no** form of this command.

hw-module module [*slot-number*] **logging onboard** [**message level** *level*]

no hw-module module [*slot-number*] **logging onboard** [**message level**]

Syntax Description

slot-number	(Optional) The slot number is always 1 and is not relevant for the ME-3400E.
message level *level*	(Optional) Specifies the severity of the hardware-related messages that are stored in the flash memory. The range is from 1 to 7 with 1 being the most severe.

Defaults

OBFL is enabled, and all messages appear.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

We recommend that you keep OBFL enabled and do not clear the data stored in the flash memory.

To ensure that the time stamps in the OBFL data logs are accurate, manually set the system clock, or configure it by using Network Time Protocol (NTP).

If you do not enter the **message level** *level* parameter, all the hardware-related messages generated by the switch are stored in the flash memory.

The optional slot number is always 1. Entering the **hw-module module** [*slot-number*] **logging onboard** [**message level** *level*] command has the same result as entering the **hw-module module logging onboard** [**message level** *level*] command.

You can verify your settings by entering the **show logging onboard** privileged EXEC command.

Examples

This example shows how to enable OBFL on a switch stack and to specify that all the hardware-related messages are stored in the flash memory:

```
Switch(config)# hw-module module logging onboard
```

This example shows how to enable OBFL on a switch and to specify that only severity 1 hardware-related messages are stored in the flash memory:

```
Switch(config)# hw-module module logging onboard message level 1
```

Related Commands

Command	Description
clear logging onboard	Removes the OBFL data in the flash memory.
show logging onboard	Displays OBFL information.

interface port-channel

To access or create the port-channel logical interface, use the **interface port-channel** command in global configuration mode. To remove the port-channel, use the **no** form of this command.

interface port-channel *port-channel-number*

no interface port-channel *port-channel-number*

Syntax Description

port-channel-number	Port-channel number. The range is 1 to 26.

Defaults

No port-channel logical interfaces are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

For Layer 2 EtherChannels, you do not have to create a port-channel interface first before assigning a physical port to a channel group. Instead, you can use the **channel-group** interface configuration command. It automatically creates the port-channel interface when the channel group gets its first physical port. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number,* or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

Note EtherChannels are not supported on ports configured with Ethernet flow point (EFP) service instances.

You create Layer 3 port channels by using the **interface port-channel** command followed by the **no switchport** interface configuration command. You should manually configure the port-channel logical interface before putting the interface into the channel group.

Only one port channel in a channel group is allowed.

Caution When using a port-channel interface as a routed port, do not assign Layer 3 addresses on the physical ports that are assigned to the channel group.

Caution Do not assign bridge groups on the physical ports in a channel group used as a Layer 3 port-channel interface because it creates loops. You must also disable spanning tree.

If you want to use the Cisco Discovery Protocol (CDP), you must configure it only on the physical port and not on the port-channel interface.

For a complete list of configuration guidelines, see the "Configuring EtherChannels" chapter in the software configuration guide for this release.

You can verify your setting by entering the **show running-config** privileged EXEC or **show etherchannel** *channel-group-number* **detail** privileged EXEC command.

Examples

This example shows how to create a port-channel interface with a port channel number of 5:

```
Switch(config)# interface port-channel 5
```

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group.
show etherchannel	Displays EtherChannel information for a channel.
show running-config	Displays the operating configuration.

interface range

To enter interface range configuration mode and to execute a command on multiple ports at the same time, use the **interface range** command in global configuration mode. To remove an interface range, use the **no** form of this command.

interface range {*port-range* | **macro** *name*}

no interface range {*port-range* | **macro** *name*}

Syntax Description

port-range	Port range. For a list of valid values for *port-range*, see the "Usage Guidelines" section.
macro *name*	Specifies the name of a macro.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When you enter interface range configuration mode, all interface parameters you enter are attributed to all interfaces within the range.

For VLANs, you can use the **interface range** command only on existing VLAN switch virtual interfaces (SVIs). To display VLAN SVIs, enter the **show running-config** privileged EXEC command. VLANs not displayed cannot be used in the **interface range** command. The commands entered under **interface range** command are applied to all existing VLAN SVIs in the range.

All configuration changes made to an interface range are saved to NVRAM, but the interface range itself is not saved to NVRAM.

You can enter the interface range in two ways:

- Specifying up to five interface ranges
- Specifying a previously defined interface-range macro

All interfaces in a range must be the same type; that is, all Fast Ethernet ports, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs. However, you can define up to five interface ranges with a single command, with each range separated by a comma.

Valid values for *port-range* type and interface:

- **vlan** *vlan-ID - vlan-ID*, where VLAN ID is from 1 to 4094

- **gigabitethernet** *module*/{*first port*} - {*last port*}, where module is always **0**
- **tengigabitethernet** *module*/{*first port*} - {*last port*}, where module is always **0**

  For physical interfaces:

  - module is always 0
  - the range is *type* **0/***number* - *number* (for example, **gigabitethernet0/1 - 2**)
- **port-channel** *port-channel-number* - *port-channel-number*, where *port-channel-number* is from 1 to 48

Note When you use the **interface range** command with port channels, the first and last port channel number in the range must be active port channels.

When you define a range, you must enter a space between the first entry and the hyphen (-):

```
interface range gigabitethernet0/1 -2
```

When you define multiple ranges, you must still enter a space after the first entry and before the comma (,):

```
interface range tengigabitetherne0/1 - 2, gigabitethernet0/1 - 2
```

You cannot specify both a macro and an interface range in the same command.

A single interface can also be specified in *port-range* (this would make the command similar to the **interface** *interface-id* global configuration command).

Note For more information about configuring interface ranges, see the software configuration guide for this release.

Examples

This example shows how to use the **interface range** command to enter interface range configuration mode to apply commands to two ports:

```
Switch(config)# interface range gigabitethernet0/1 - 2
Switch(config-if-range)#
```

This example shows how to use a port-range macro *macro1* for the same function. The advantage is that you can reuse *macro1* until you delete it.

```
Switch(config)# define interface-range macro1 gigabitethernet0/1 - 2
Switch(config)# interface range macro macro1
Switch(config-if-range)#
```

Related Commands

Command	Description
define interface-range	Creates an interface range macro.
show running-config	Displays the operating configuration.

interface vlan

To create or access a switch virtual interface (SVI) and to enter interface configuration mode, use the **interface vlan** command in global configuration mode. To delete an SVI, use the **no** form of this command.

interface vlan *vlan-id*

no interface vlan *vlan-id*

Syntax Description

vlan-id	VLAN number. The range is 1 to 4094.

Defaults

The default VLAN interface is VLAN 1.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

SVIs are created the first time that you enter the **interface vlan** *vlan-id* command for a particular *vlan*. The *vlan-id* corresponds to the VLAN-tag associated with data frames on an IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port.

Note When you create an SVI, it does not become active until it is associated with a physical port.

If you delete an SVI by entering the **no interface vlan** *vlan-id* command, the deleted interface is no longer visible in the output from the **show interfaces** privileged EXEC command.

Note You cannot delete the VLAN 1 interface.

You can reinstate a deleted SVI by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but much of the previous configuration will be gone.

You can verify your setting by entering the **show interfaces** and **show interfaces vlan** *vlan-id* privileged EXEC commands.

Examples

This example shows how to create VLAN ID 23 and enter interface configuration mode:

```
Switch(config)# interface vlan 23
Switch(config-if)#
```

Related Commands

Command	Description
show interfaces vlan *vlan-id*	Displays the administrative and operational status of all interfaces or the specified VLAN.

ip access-group

To control access to a Layer 2 or Layer 3 interface, use the **ip access-group** command in interface configuration mode.To remove all access groups or the specified access group from the interface, use the **no** form of this command.

ip access-group {*access-list-number* | *name*} {**in** | **out**}

no ip access-group [*access-list-number* | *name*] {**in** | **out**}

Note You cannot attach an ACL to a Layer 2 port that has an Ethernet flow point (EFP) service instance configured on it. The **ip access-group** command is rejected on these ports.

Syntax Description

access-list-number	The number of the IP access control list (ACL). The range is 1 to 199 or 1300 to 2699.
name	The name of an IP ACL, specified in the **ip access-list** global configuration command.
in	Specifies filtering on inbound packets.
out	Specifies filtering on outbound packets. This keyword is valid only on Layer 3 interfaces.

Defaults

No access list is applied to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can apply named or numbered standard or extended IP access lists to an interface. To define an access list by name, use the **ip access-list** global configuration command. To define a numbered access list, use the **access list** global configuration command. You can used numbered standard access lists ranging from 1 to 99 and 1300 to 1999 or extended access lists ranging from 100 to 199 and 2000 to 2699.

You can use this command to apply an access list to a Layer 2 interface (port ACL) or Layer 3 interface. However, note these limitations for port ACLs:

- You can only apply ACLs in the inbound direction; the **out** keyword is not supported for Layer 2 interfaces.
- You cannot apply an ACL to a port configured with a service instance. Layer 2 ACLs are not supported on these ports.
  - If you try to configure a service instance on a port that has a port ACL attached, the service port configuration is rejected with a warning message.
  - If you try to attach a port ACL to a port that has a service instance, the configuration is rejected with a warning message.
- You can only apply one IP ACL and one MAC ACL per interface.
- Port ACLs do not support logging; if the **log** keyword is specified in the IP ACL, it is ignored.
- An IP ACL applied to a Layer 2 interface only filters IP packets. To filter non-IP packets, use the **mac access-group** interface configuration command with MAC extended ACLs.

You can use router ACLs, input port ACLs, and VLAN maps on the same switch. However, a port ACL always takes precedence. When both an input port ACL and a VLAN map are applied, incoming packets received on ports with the port ACL applied are filtered by the port ACL. Other packets are filtered by the VLAN map.

- When an input port ACL is applied to an interface and a VLAN map is applied to a VLAN that the interface is a member of, incoming packets received on ports with the ACL applied are filtered by the port ACL. Other packets are filtered by the VLAN map.
- When an input router ACL and input port ACLs exist in an switch virtual interface (SVI), incoming packets received on ports to which a port ACL is applied are filtered by the port ACL. Incoming routed IP packets received on other ports are filtered by the router ACL. Other packets are not filtered.
- When an output router ACL and input port ACLs exist in an SVI, incoming packets received on the ports to which a port ACL is applied are filtered by the port ACL. Outgoing routed IP packets are filtered by the router ACL. Other packets are not filtered.
- When a VLAN map, input router ACLs, and input port ACLs exist in an SVI, incoming packets received on the ports to which a port ACL is applied are only filtered by the port ACL. Incoming routed IP packets received on other ports are filtered by both the VLAN map and the router ACL. Other packets are filtered only by the VLAN map.
- When a VLAN map, output router ACLs, and input port ACLs exist in an SVI, incoming packets received on the ports to which a port ACL is applied are only filtered by the port ACL. Outgoing routed IP packets are filtered by both the VLAN map and the router ACL. Other packets are filtered only by the VLAN map.
- VLAN maps are applied to all switchports that belong to the VLAN, as well as EFPs with a bridge domain equal to the VLAN.

You can apply IP ACLs to both outbound or inbound Layer 3 interfaces.

A Layer 3 interface can have one IP ACL applied in each direction.

You can configure only one VLAN map and one router ACL in each direction (input/output) on a VLAN interface.

For standard inbound access lists, after the switch receives a packet, it checks the source address of the packet against the access list. IP extended access lists can optionally check other fields in the packet, such as the destination IP address, protocol type, or port numbers. If the access list permits the packet,

the switch continues to process the packet. If the access list denies the packet, the switch discards the packet. If the access list has been applied to a Layer 3 interface, discarding a packet (by default) causes the generation of an Internet Control Message Protocol (ICMP) Host Unreachable message. ICMP Host Unreachable messages are not generated for packets discarded on a Layer 2 interface.

For standard outbound access lists, after receiving a packet and sending it to a controlled interface, the switch checks the packet against the access list. If the access list permits the packet, the switch sends the packet. If the access list denies the packet, the switch discards the packet and, by default, generates an ICMP Host Unreachable message.

If the specified access list does not exist, all packets are passed.

You can verify your settings by entering the **show ip interface, show access-lists,** or **show ip access-lists** privileged EXEC command.

Examples

This example shows how to apply IP access list 101 to inbound packets on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 101 in
```

Related Commands

Command	Description
access list	Configures a numbered ACL.
ip access-list	Configures a named ACL.
show access-lists	Displays ACLs configured on the switch.
show ip access-lists	Displays IP ACLs configured on the switch.
show ip interface	Displays information about interface status and configuration.

ip address

To set an IP address for the Layer 2 switch or to set an IP address for each switch virtual interface (SVI) or routed port on the Layer 3 switch, use the **ip address** command in interface configuration mode. To remove an IP address or to disable IP processing, use the **no** form of this command.

ip address *ip-address subnet-mask* [**secondary**]

no ip address [*ip-address subnet-mask*] [**secondary**]

Syntax Description

ip-address	IP address.
subnet-mask	Mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.

Defaults

No IP address is defined.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If you remove the switch IP address through a Telnet session, your connection to the switch will be lost.

Hosts can find subnet masks using the Internet Control Message Protocol (ICMP) Mask Request message. Routers respond to this request with an ICMP Mask Reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the switch detects another host using one of its IP addresses, it will send an error message to the console.

You can use the optional keyword **secondary** to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and ARP requests are handled properly, as are interface routes in the IP routing table.

Note If any router on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.

When you are routing Open Shortest Path First (OSPF), ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

If your switch receives its IP address from a Bootstrap Protocol (BOOTP) or a DHCP server and you remove the switch IP address by using the **no ip address** command, IP processing is disabled, and the BOOTP or the DHCP server cannot reassign the address.

You can verify your settings by entering the **show running-config** privileged EXEC command.

Examples

This example shows how to configure the IP address for the Layer 2 switch on a subnetted network:

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

This example shows how to configure the IP address for a Layer 3 port on the switch:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.

ip igmp filter

To control whether or not all hosts on a Layer 2 interface can join one or more IP multicast groups by applying an Internet Group Management Protocol (IGMP) profile to the interface, use the **ip igmp filter** command in interface configuration mode. To remove the specified profile from the interface, use the **no** form of this command.

ip igmp filter *profile number*

no ip igmp filter

Syntax Description

profile number	The IGMP profile number to be applied. The range is 1 to 4294967295.

Defaults

No IGMP filters are applied.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can apply IGMP filters only to Layer 2 physical interfaces.

You cannot apply IGMP filters to routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.

An IGMP profile can be applied to one or more switch port interfaces, but one port can have only one profile applied to it.

You can verify your setting by using the **show running-config** privileged EXEC command and by specifying an interface.

Examples

This example shows how to apply IGMP profile 22 to a port.

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp filter 22
```

Related Commands

Command	Description
ip igmp profile	Configures the specified IGMP profile number.
show ip igmp profile	Displays the characteristics of the specified IGMP profile.
show running-config interface *interface-id*	Displays the running configuration on the switch interface, including the IGMP profile (if any) that is applied to an interface.

ip igmp max-groups

To set the maximum number of Internet Group Management Protocol (IGMP) groups that a Layer 2 interface can join, or to configure the IGMP throttling action when the maximum number of entries is in the forwarding table, use the **ip igmp max-groups** command in interface configuration mode. To set the maximum back to the default, which is to have no maximum limit, or to return to the default throttling action, which is to drop the report, use the **no** form of this command.

ip igmp max-groups {*number* | **action** {**deny** | **replace**}}

no ip igmp max-groups {*number* | **action**}

Syntax Description

number	The maximum number of IGMP groups that an interface can join. The range is 0 to 4294967294. The default is no limit.
action deny	When the maximum number of entries is in the IGMP snooping forwarding table, drops the next IGMP join report. This is the default action.
action replace	When the maximum number of entries is in the IGMP snooping forwarding table, replaces the existing group with the new group for which the ICMP report was received.

Defaults

The default maximum number of groups is no limit.

After the switch learns the maximum number of IGMP group entries on an interface, the default throttling action is to drop the next IGMP report that the interface receives and to not add an entry for the IGMP group to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can use this command only on Layer 2 physical interfaces and on logical EtherChannel interfaces.

You cannot set IGMP maximum groups for routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.

Follow these guidelines when configuring the IGMP throttling action:

- If you configure the throttling action as **deny** and set the maximum group limitation, the entries that were previously in the forwarding table are not removed but are aged out. After these entries are aged out, when the maximum number of entries is in the forwarding table, the switch drops the next IGMP report received on the interface.

- If you configure the throttling action as **replace** and set the maximum group limitation, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the switch replaces a randomly-selected multicast entry with the received IGMP report.
- When the maximum group limitation is set to the default (no maximum), entering the **ip igmp max-groups** {**deny | replace**} command has no effect.

You can verify your setting by using the **show running-config** privileged EXEC command and by specifying an interface.

Examples

This example shows how to limit to 25 the number of IGMP groups that a port can join.

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp max-groups 25
```

This example shows how to configure the switch to replace the existing group with the new group for which the IGMP report was received when the maximum number of entries is in the forwarding table:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip igmp max-groups action replace
```

Related Commands

Command	Description
show running-config interface *interface-id*	Displays the running configuration on the switch interface, including the maximum number of IGMP groups that an interface can join and the throttling action.

ip igmp profile

To create an Internet Group Management Protocol (IGMP) profile and enter IGMP profile configuration mode, use the **ip igmp profile** command in global configuration mode. In enter IGMP profile configuration mode, you can specify the configuration of the IGMP profile to be used for filtering IGMP membership reports from a switchport. To delete the IGMP profile, use the **no** form of this command.

ip igmp profile *profile number*

no ip igmp profile *profile number*

Syntax Description

profile number	The IGMP profile number being configured. The range is 1 to 4294967295.

Defaults

No IGMP profiles are defined. When configured, the default action for matching an IGMP profile is to deny matching addresses.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When you are in IGMP profile configuration mode, you can create the profile by using these commands:

- **deny**: specifies that matching addresses are denied; this is the default condition.
- **exit**: exits from igmp-profile configuration mode.
- **no**: negates a command or resets to its defaults.
- **permit**: specifies that matching addresses are permitted.
- **range**: specifies a range of IP addresses for the profile. This can be a single IP address or a range with a start and an end address.

  When entering a range, enter the low IP multicast address, a space, and the high IP multicast address.

You can apply an IGMP profile to one or more Layer 2 interfaces, but each interface can have only one profile applied to it.

You can verify your settings by using the **show ip igmp profile** privileged EXEC command.

Examples

This example shows how to configure IGMP profile 40 that permits the specified range of IP multicast addresses.

```
Switch(config)# ip igmp profile 40
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

Related Commands

Command	Description
ip igmp filter	Applies the IGMP profile to the specified interface.
show ip igmp profile	Displays the characteristics of all IGMP profiles or the specified IGMP profile number.

ip igmp snooping

To globally enable Internet Group Management Protocol (IGMP) snooping on the switch or to enable it on a per-VLAN basis, use the **ip igmp snooping** command in global configuration mode. To return to the default setting, use the **no** form of this command.

ip igmp snooping [**vlan** *vlan-id*]

no ip igmp snooping [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Enables IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.

Defaults

IGMP snooping is globally enabled on the switch.

IGMP snooping is enabled on VLAN interfaces.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When IGMP snooping is enabled globally, it is enabled in all the existing VLAN interfaces. When IGMP snooping is disabled globally, it is disabled on all the existing VLAN interfaces.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Examples

This example shows how to globally enable IGMP snooping:

```
Switch(config)# ip igmp snooping
```

This example shows how to enable IGMP snooping on VLAN 1:

```
Switch(config)# ip igmp snooping vlan 1
```

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays the snooping configuration.
show ip igmp snooping groups	Displays IGMP snooping multicast information.
show ip igmp snooping mrouter	Displays the IGMP snooping router ports.

ip igmp snooping last-member-query-interval

To enable the Internet Group Management Protocol (IGMP) configurable-leave timer globally or on a per-VLAN basis, use the **ip igmp snooping last-member-query-interval** command in global configuration command. To the default setting, use the **no** form of this command to return.

ip igmp snooping [**vlan** *vlan-id*] **last-member-query-interval** *time*

no ip igmp snooping [**vlan** *vlan-id*] **last-member-query-interval**

Syntax Descriptiont

vlan *vlan-id*	(Optional) Enables IGMP snooping and the leave timer on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
time	Interval time out in seconds. The range is 100 to 32768 milliseconds.

Defaults

The default timeout setting is 1000 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When IGMP snooping is globally enabled, IGMP snooping is enabled on all the existing VLAN interfaces. When IGMP snooping is globally disabled, IGMP snooping is disabled on all the existing VLAN interfaces.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Configuring the leave timer on a VLAN overrides the global setting.

The IGMP configurable leave time is only supported on devices running IGMP Version 2.

The configuration is saved in NVRAM.

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Examples

This example shows how to globally enable the IGMP leave timer for 2000 milliseconds:

```
Switch(config)# ip igmp snooping last-member-query-interval 2000
```

This example shows how to configure the IGMP leave timer for 3000 milliseconds on VLAN 1:

```
Switch(config)# ip igmp snooping vlan 1 last-member-query-interval 3000
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
show ip igmp snooping	Displays the IGMP snooping configuration.

ip igmp snooping report-suppression

To enable Internet Group Management Protocol (IGMP) report suppression, use the **ip igmp snooping report-suppression** command in global configuration mode. To disable IGMP report suppression and to forward all IGMP reports to multicast routers, u se the **no** form of this command.

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Defaults

IGMP report suppression is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The switch uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP router suppression is enabled (the default), the switch sends the first IGMP report from all hosts for a group to all the multicast routers. The switch does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the switch forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the switch forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression by entering the **no ip igmp snooping report-suppression** command, all IGMP reports are forwarded to all the multicast routers.

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Examples

This example shows how to disable report suppression:

```
Switch(config)# no ip igmp snooping report-suppression
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN.

ip igmp snooping tcn

To configure the Internet Group Management Protocol (IGMP) Topology Change Notification (TCN) behavior, use the **ip igmp snooping tcn** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip igmp snooping tcn {**flood query count** *count* | **query solicit**}

no ip igmp snooping tcn {**flood query count** | **query solicit**}

Syntax Description

flood query count *count*	Specifies the number of IGMP general queries for which the multicast traffic is flooded. The range is 1 to 10.
query solicit	Sends an IGMP leave message (global leave) to speed the process of recovering from the flood mode caused during a TCN event.

Defaults

The TCN flood query count is 2.

The TCN query solicitation is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can prevent the loss of the multicast traffic that might occur because of a topology change by using this command. If you set the TCN flood query count to 1 by using the ip **igmp snooping tcn flood query count** command, the flooding stops after receiving one general query. If you set the count to 7, the flooding of multicast traffic due to the TCN event lasts until seven general queries are received. Groups are relearned based on the general queries received during the TCN event.

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Examples

This example shows how to specify 7 as the number of IGMP general queries for which the multicast traffic is flooded:

```
Switch(config)# no ip igmp snooping tcn flood query count 7
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping tcn flood	Specifies flooding on an interface as the IGMP snooping spanning-tree TCN behavior.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN.

ip igmp snooping tcn flood

To specify multicast flooding as the Internet Group Management Protocol (IGMP) snooping spanning-tree Topology Change Notification (TCN) behavior, use the **ip igmp snooping tcn flood** command in interface configuration mode. To disable the multicast flooding, use the **no** form of this command.

ip igmp snooping tcn flood

no ip igmp snooping tcn flood

Syntax Description

This command has no arguments or keywords.

Defaults

Multicast flooding is enabled on an interface during a spanning-tree TCN event.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When the switch receives a TCN, multicast traffic is flooded to all the ports until two general queries are received. If the switch has many ports with attached hosts that are subscribed to different multicast groups, this flooding behavior might not be desirable because the flooded traffic might exceed the capacity of the link and cause packet loss.

You can change the flooding query count by using the **ip igmp snooping tcn flood query count** *count* global configuration command.

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Examples

This example shows how to disable the multicast flooding on an interface:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no ip igmp snooping tcn flood
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping on the switch or on a VLAN.
ip igmp snooping tcn	Configures the IGMP TCN behavior on the switch.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN.

ip igmp snooping vlan immediate-leave

To enable Internet Group Management Protocol (IGMP) snooping immediate-leave processing on a per-VLAN basis, use the **ip igmp snooping vlan** *vlan-id* **immediate-leave** command in global configuration mode.To return to the default setting, use the **no** form of this command.

ip igmp snooping vlan *vlan-id* **immediate-leave**

no ip igmp snooping vlan *vlan-id* **immediate-leave**

Syntax Description

vlan-id	Enable IGMP snooping and the Immediate-Leave feature on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.

Defaults

IGMP immediate-leave processing is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

You should only configure the Immediate Leave feature when there is a maximum of one receiver on every port in the VLAN. The configuration is saved in NVRAM.

The Immediate Leave feature is supported only with IGMP Version 2 hosts.

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Examples

This example shows how to enable IGMP immediate-leave processing on VLAN 1:

```
Switch(config)# ip igmp snooping vlan 1 immediate-leave
```

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays the snooping configuration.
show ip igmp snooping groups	Displays IGMP snooping multicast information.
show ip igmp snooping mrouter	Displays the IGMP snooping router ports.
show ipc detail	Displays the configuration and operation information for the IGMP querier configured on a switch.

ip igmp snooping vlan mrouter

To add a multicast router port or to configure the multicast learning method, use the **ip igmp snooping vlan** *vlan-id* **mrouter** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id* | **learn pim-dvmrp**}

no ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id* | **learn pim-dvmrp**}

Note Though visible in the command-line help strings, the cgmp keyword is not supported.

Syntax Description

vlan-id	Enables IGMP snooping, and add the port in the specified VLAN as the multicast router port. The range is 1 to 1001 and 1006 to 4094.
interface *interface-id*	Specifies the next-hop interface to the multicast router. Valid interfaces are physical interfaces and port channels. The port-channel range is 1 to 48.
learn pim-dvmrp	Specifies the multicast router learning method. The only learning method supported on the Cisco ME switch is **pim-dvmrp**, which sets the switch to learn multicast router ports by snooping on IGMP queries and Protocol-Independent Multicast-Distance Vector Multicast Routing Protocol (PIM-DVMRP) packets.

Defaults

By default, there are no multicast router ports.

The default learning method is **pim-dvmrp**—to snoop IGMP queries and PIM-DVMRP packets.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

The configuration is saved in NVRAM.

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Examples

This example shows how to configure a port as a multicast router port:

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet0/2
```

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays the snooping configuration.
show ip igmp snooping groups	Displays IGMP snooping multicast information.
show ip igmp snooping mrouter	Displays the IGMP snooping router ports.
show ipc detail	Displays the configuration and operation information for the IGMP querier configured on a switch.

ip igmp snooping vlan static

To enable Internet Group Management Protocol (IGMP) snooping and to statically add a Layer 2 port as a member of a multicast group, use the **ip igmp snooping vlan** *vlan-id* **static** command in global configuration mode. To remove ports specified as members of a static multicast group, use the **no** form of this command.

ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

no ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

Syntax Description

vlan-id	Enables IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
ip-address	Adds a Layer 2 port as a member of a multicast group with the specified group IP address.
interface *interface-id*	Specifies the interface of the member port. The keywords have these meanings: • **gigabitethernet** *interface number*—a Gigabit Ethernet IEEE 802.3z interface. • **Tengigabitethernet** *interface number*—a 10-Gigabit Ethernet interface. • **port-channel** *interface number*—a channel interface. The range is 0 to 26.

Defaults

By default, there are no ports statically configures as members of a multicast group.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

The configuration is saved in NVRAM.

Examples

This example shows how to statically configure a port as a multicast router port:

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet0/2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

Related Commands

Command	Description
ip igmp snooping report-suppression	Enables IGMP report suppression.
show ip igmp snooping	Displays the snooping configuration.
show ip igmp snooping groups	Displays IGMP snooping multicast information.
show ip igmp snooping mrouter	Displays the IGMP snooping router ports.
show ipc detail	Displays the configuration and operation information for the IGMP querier configured on a switch.

ip sla

To begin configuring a Cisco IOS IP Service Level Agreements (SLAs) operation and enter IP SLA configuration mode, use the ip slacommand in global configuration mode. To remove all configuration information for an operation, including the schedule of the operation, reaction configuration, and reaction triggers, use the no form of this command.

ip sla *operation-number*

no ip sla *operation-number*

Syntax Description

operation-number	Operation number used for the identification of the IP SLAs operation you want to configure.

Defaults

No IP SLAs operation is configured.

Command Modes

Global configuration

Command History

Release	Modification
15.2(4)S1	This command was introduced.

Usage Guidelines

The **ip sla** command is used to begin configuration for an IP SLAs operation. Use this command to specify an identification number for the operation you are about to configure. After you enter this command, the router will enter IP SLA configuration mode.

The **ip sla** command is supported in IPv4 networks. This command can also be used when configuring an IP SLAs operation that supports IPv6 addresses.

IP SLAs allows a maximum of 2000 operations.

Debugging is supported only on the first 32 operation numbers.

After you configure an operation, you must schedule the operation. For information on scheduling an operation, refer to the **ip sla schedule** and **ip sla group schedule** global configuration commands. You can also optionally set reaction triggers for the operation. For information on reaction triggers, refer to the **ip sla reaction-configuration** and **ip sla reaction-trigger** global configuration commands.

To change the operation type of an existing IP SLAs operation, you must first delete the IP SLAs operation (using the **no ip sla**) and then reconfigure the operation with the new operation type.

Note After you schedule an operation, you cannot modify the configuration of the operation. To modify the configuration of the operation after it is scheduled, you must first unschedule the IP SLAs operation (using the **no ip sla** command) and then reconfigure the operation with the new operation parameters.

To display the current configuration settings of the operation, use the **show ip sla configuration** command in user EXEC or privileged EXEC mode.

Examples

In the following example, operation 99 is configured as a UDP jitter operation in an IPv4 network and scheduled to start running in 5 hours. The example shows the **ip sla** command being used in an IPv4 network.

```
Switch(config-term)# ip sla 99
Switch(config-ip-sla)# udp-jitter 172.29.139.134 dest-port 5000 num-packets 20
Switch(config-ip-sla)# ip sla schedule 99 life 300 start-time after 00:05:00
```

Note If operation 99 already exists and has not been scheduled, the command line interface will enter IP SLA configuration mode for operation 99. If the operation already exists and has been scheduled, this command will fail.

Related Commands

Command	Description
ip sla group schedule	Configures the group scheduling parameters for multiple IP SLAs operations.
ip sla reaction-configuration	Configures certain actions to occur based on events under the control of IP SLAs.
ip sla reaction-trigger	Defines a second IP SLAs operation to make the transition from a pending state to an active state when one of the trigger action type options are defined with the **ip sla reaction-configuration** command.
ip sla schedule	Configures the scheduling parameters for a single IP SLAs operation.
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.
show ip sla statistics	Displays the current operational status and statistics of all IP SLAs operations or a specified operation.
show ip sla statistics aggregated	Displays the aggregated statistical errors and distribution information for all IP SLAs operations or a specified operation.

ip sla reaction-configuration

To configure proactive threshold monitoring parameters for an IP Service Level Agreements (SLAs) operation, use the **ip sla reaction-configuration** command in global configuration mode. To disable all the threshold monitoring configuration for a specified IP SLAs operation, use the **no** form of this command.

ip sla reaction-configuration *operation-number* {**react** {**unavailableDS** | **unavailableSD** }{**loss-ratioDS** | **loss-ratioSD**}[**threshold-type** {**average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** }] [**threshold-value** *upper-threshold lower-threshold*]]

no ip sla reaction-configuration *operation-number* [**react** *monitored-element*]

Syntax Description

operation-number	Number of the IP SLAs operation for which reactions are to be configured.
react	Specifies the element to be monitored for threshold violations. **Note** The elements supported for monitoring will vary depending on the type of IP SLAs operation you are running. See the Usage Guidelines for information.
unavailableDS	Specifies that a reaction should occur if the percentage of destination-to-source Frame Loss Ratio (FLR) violates the upper threshold or lower threshold.
unavailableSD	Specifies that a reaction should occur if the percentage of source-to-destination FLR violates the upper threshold or lower threshold.
loss-ratioDS	Specifies that a reaction should occur if the one-way destination-to-source loss-ratio violates the upper threshold or lower threshold.
loss-ratioSD	Specifies that a reaction should occur if the one way source-to-destination loss-ratio violates the upper threshold or lower threshold.
threshold-type average [*number-of-measurements*]	(Optional) When the average of a specified number of measurements for the monitored element exceeds the upper threshold or when the average of a specified number of measurements for the monitored element drops below the lower threshold, perform the action defined by the action-type keyword. For example, if the upper threshold for **reactrtttthreshold-typeaverage3** is configured as 5000 ms and the last three results of the operation are 6000, 6000, and 5000 ms, the average would be 6000 + 6000 + 5000 = 17000/3 = 5667, thus violating the 5000 ms upper threshold. The default number of 5 averaged measurements can be changed using the number-of-measurements argument. The valid range is from 1 to 16.
threshold-type consecutive [*occurrences*]	(Optional) When a threshold violation for the monitored element is met consecutively for a specified number of times, perform the action defined by the action-type keyword. The default number of 5 consecutive occurrences can be changed using the occurrences argument. The valid range is from 1 to 16. The occurrences value will appear in the output of the **show ip sla reaction-configuration** command as the "Threshold Count" value.
threshold-type immediate	(Optional) When a threshold violation for the monitored element is met, immediately perform the action defined by the action-type keyword.

threshold-type never	(Optional) Do not calculate threshold violations. This is the default threshold type.
threshold-value *upper-threshold* l*ower-threshold*	Optional) Specifies the upper-threshold and lower-threshold values of the applicable monitored elements. See the Default Threshold Values for Monitored Elements table in the "Usage Guidelines" section for a list of the default values.

Defaults

IP SLAs proactive threshold monitoring is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(4)S1	This command was introduced.

Usage Guidelines

You can configure the **ip sla reaction-configuration** command multiple times to enable proactive threshold monitoring for multiple elements, such as configuring thresholds for both destination-to-source packet loss and MOS for the same operation. However, disabling individual monitored elements is not supported. The **no ip sla reaction-configuration** command disables all proactive threshold monitoring configuration for the specified IP SLAs operation.

The keyword options for this command are not case sensitive. The keywords in online help for the **action-type**option and **react** *monitored-element* keyword and argument combinations contain uppercase letters to enhance readability only.

The **never** keyword option for the **threshold-type** keyword does not work with the **unavailableDS** and **unavailableSD** monitored elements for measuring Ethernet Frame Loss Ratio (FLR).

Not all elements can be monitored by all IP SLAs operations. If you attempt to configure an unsupported monitored-element, such as MOS for a UDP echo operation, the following message displays:

```
Invalid react option for the Probe type configured
```

Examples

The following example shows how to configure IP SLAs operation 1:

```
Switch(config)# ip sla reaction-configuration 1 react loss-ratioSD threshold-type
immediate threshold-value 55 50
```

Related Commands

Command	Description

Command	Description

ip sla schedule

To configure the scheduling parameters for a single Cisco IOS IP Service Level Agreements (SLAs) operation, use the ip sla schedulecommand in global configuration mode. To stop the operation and place it in the default state (pending), use the no form of this command.

ip sla schedule *operation-number* [**life** {**forever** | *seconds*}] [**start-time** {*hh : mm* [*: ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh : mm : ss*}] [**ageout** *seconds*] [**recurring**]

no ip sla schedule *operation-number*

Syntax Description

operation-number	Number of the IP SLAs operation to schedule.
life forever	(Optional) Schedules the operation to run indefinitely.
life *seconds*	(Optional) Number of seconds the operation actively collects information. The default is 3600 seconds (one hour).
start-time	(Optional) Time when the operation starts.
hh : mm [*: ss*]	Specifies an absolute start time using hour, minute, and (optionally) second. Use the 24-hour clock notation. For example, start-time 01:02 means "start at 1:02 a.m.," and start-time 13:01:30 means "start at 1:01 p.m. and 30 seconds." The current day is implied unless you specify a month and day.
month	(Optional) Name of the month to start the operation in. If month is not specified, the current month is used. Use of this argument requires that a day be specified. You can specify the month by using either the full English name or the first three letters of the month.
day	(Optional) Number of the day (in the range 1 to 31) to start the operation on. If a day is not specified, the current day is used. Use of this argument requires that a month be specified.
pending	(Optional) No information is collected. This is the default value.
after *hh : mm : ss*	(Optional) Indicates that the operation should start hh hours, mm minutes, and ss seconds after this command was entered.
ageout *seconds*	(Optional) Number of seconds to keep the operation in memory when it is not actively collecting information. The default is 0 seconds (never ages out).
recurring	(Optional) Indicates that the operation will start automatically at the specified time and for the specified duration every day.

Defaults

The operation is placed in a pending state (that is, the operation is enabled but not actively collecting information).

Command Modes

Global configuration

Command History

Release	Modification
15.2(4)S1	This command was introduced.

Usage Guidelines

After you schedule the operation with the **ip sla schedule** command, you cannot change the configuration of the operation. To change the configuration of the operation, use the **no** form of the i**p sla** global configuration command and reenter the configuration information.

If the operation is in a pending state, you can define the conditions under which the operation makes the transition from pending to active with the ip sla reaction-trigger and ip sla reaction-configuration global configuration commands. When the operation is in an active state, it immediately begins collecting information.

The following time line shows the age-out process of the operation:

W----------X----------Y----------Z

where:

- W is the time the operation was configured with the **ip sla** global configuration command.
- X is the start time or start of life of the operation (that is, when the operation became "active").
- Y is the end of life as configured with the **ip sla schedule** global configuration command (life seconds have counted down to zero).
- Z is the age out of the operation.

Age out starts counting down at W and Y, is suspended between X and Y, and is reset to its configured size at Y.

The operation to can age out before it executes (that is, Z can occur before X). To ensure that this does not happen, configure the difference between the operation's configuration time and start time (X and W) to be less than the age-out seconds.

Note The total RAM required to hold the history and statistics tables is allocated at the time of scheduling the IP SLAs operation. This prevents router memory problems when the router gets heavily loaded and lowers the amount of overhead an IP SLAs operation causes on a router when it is active.

The **recurring** keyword is supported only for scheduling single IP SLAs operations. You cannot schedule multiple IP SLAs operations using the **ip sla schedule** command. The **life** value for a recurring IP SLAs operation should be less than one day. The **ageout** value for a recurring operation must be "never" (which is specified with the value 0), or the sum of the **life** and **ageout** values must be more than one day. If the **recurring** option is not specified, the operations are started in the existing normal scheduling mode.

The **ip sla schedule** command is supported in IPv4 networks. This command can also be used when configuring an IP SLAs operation that supports IPv6 addresses.

Examples

In the following example, operation 25 begins actively collecting data at 3:00 p.m. on April 5. This operation will age out after 12 hours of inactivity, which can be before it starts or after it has finished with its life. When this operation ages out, all configuration information for the operation is removed (that is, the configuration information is no longer in the running configuration in RAM).

```
ip sla schedule 25 life 43200 start-time 15:00 apr 5 ageout 43200
```

In the following example, operation 1 begins collecting data after a 5-minute delay:

```
ip sla schedule 1 start-time after 00:05:00
```

In the following example, operation 3 begins collecting data immediately and is scheduled to run indefinitely:

```
ip sla schedule 3 start-time now life forever
```

In the following example, operation 15 begins automatically collecting data every day at 1:30 a.m.:

```
ip sla schedule 15 start-time 01:30:00 recurring
```

Related Commands

Command	Description
ip sla	Begins configuration for an IP SLAs operation and enters IP SLA configuration mode.
ip sla group schedule	Configures the group scheduling parameters for multiple IP SLAs operations.
ip sla reaction-configuration	Configures certain actions to occur based on events under the control of IP SLAs.
show ip sla configuration	Displays configuration values including all defaults for all IP SLAs operations or the specified operation.

ip ssh

To configure the switch to run Secure Shell (SSH) Version 1 or SSH Version 2, use the **ip ssh** global configuration command. To return to the default setting, use the **no** form of this command.

ip ssh version [**1** | **2**]

no ip ssh version [**1** | **2**]

This command is available only when your switch is running the cryptographic (encrypted) software image.

Syntax Description

1	(Optional) Configures the switch to run SSH Version 1 (SSHv1).
2	(Optional) Configures the switch to run SSH Version 2 (SSHv1).

Defaults

The default version is the latest SSH version supported by the SSH client.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If you do not enter this command or if you do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.

The switch supports an SSHv1 or an SSHv2 server. It also supports an SSHv1 client. For more information about the SSH server and the SSH client, see the software configuration guide for this release.

A Rivest, Shamir, and Adelman (RSA) key pair generated by an SSHv1 server can be used by an SSHv2 server and the reverse.

You can verify your settings by entering the **show ip ssh** or **show ssh** privileged EXEC command.

Examples

This example shows how to configure the switch to run SSH Version 2:

```
Switch(config)# ip ssh version 2
```

Related Commands

Command	Description
show ip ssh	Displays if the SSH server is enabled and displays the version and configuration information for the SSH server.
show ssh	Displays the status of the SSH server.

l2protocol

To tunnel Layer 2 control packets as data over an Ethernet flow point (EFP) service instance or to allow Layer 2 protocols to peer over an interface configured with a service instance, use the **l2protocol** command in service-instance configuration mode. To remove the configuration, use the **no** form of the command.

l2protocol {**peer** | **tunnel**} [**cdp** | **dtp** | **lacp** | **lldp** | **pagp** | **stp** | **udld** | **vtp**]

no l2protocol {**peer** | **tunnel**} [**cdp** | **dtp** | **lacp** | **lldp** | **pagp** | **stp** | **udld** | **vtp**]

Syntax Description\

peer	Configures the EFP to allow Layer 2 protocols to peer with a neighboring switch on an EFP-enabled interface. PDUs are processed locally.
tunnel	Configures the EFP to tunnel Layer 2 control packets. Overwrites the PDU-destination MAC address with a well known Cisco propritary multicast address (01-00-0c-cd-cd-d0)
cdp	(Optional) Specifies that the switch peer or tunnel Cisco Discovery Protocol (CDP) packets.
dtp	(Optional) Specifies that the switch tunnel Dynamic Trunking Protocol (DTP) packets. This keyword is not supported with the **peer** keyword.
lacp	(Optional) Specifies that the switch peer or tunnel Link Aggregation Control Protocol (LACP) packets.
lldp	(Optional) Specifies that the switch peer or tunnel Link Layer Discovery Protocol (LLDP) packets.
pagp	(Optional) Specifies that the switch peer or tunnel Port Aggregation Protocol (PAgP) packets.
stp	(Optional) Specifies that the switch peer or tunnel Spanning Tree Protocol (STP) packets.
udld	(Optional) Specifies that the switch peer or tunnel UniDirectional Link Detection (UDLD) packets.
vtp	(Optional) Specifies that the switch tunnel VLAN Trunking Protocol (VTP) packets. This keyword is not supported with the **peer** keyword.

Defaults

The service instance does not tunnel or peer Layer 2 control packets.

Command Modes

Service-instance configuration mode.

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can enter a keyword to identify a Layer 2 control protocol. If you do not enter a protocol, all Layer 2 control protocols are peered or tunneled.

Although you can configure DTP and VTP peering, this has no effect because the switch does not support these protocols.

In ME3800X platform, Cisco IOS Release 12.2(52)EY, the **forward** keyword is not supported for the **l2protocol** command. Therefore, it is impossible to forward Layer 2 control packets from a ME3800X switch to a Cisco 7600 router and vice versa. The tunnel option in ME3800X overwrites the PDU-destination MAC address with a well-known Cisco proprietary multicast address (01-00-0c-cd-cd-d0), while the forward option in Cisco 7600 simply forwards the PDU without any change or local processing; thus, the two platforms cannot cooperate.

For example:

Peer: PDUs are processed locally

Tunnel: Overwrites the PDU-destination MAC address with a well-known Cisco proprietary multicast address (01-00-0c-cd-cd-d0)

Examples

This example shows how to configure the service instance to peer CDP with a neighbor service instance:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan none
Switch(config-if)# service instance 1 Ethernet
Switch(config-if-srv)# encapsulation untagged
Switch(config-if-srv)# l2protocol peer cdp
Switch(config-if-srv)# bridge-domain 1
Switch(config-if-srv)# exit
```

Related Commands

Command	Description
service instance	Creates a service instance on an interface.

l2 vfi

To create a virtual forwarding infrastructure (VFI) and to enter manual VFI configuration mode, use the **l2 vfi** command in global configuration mode. A VFI is a logical switching entity used to implement hierarchical virtual private LAN service (H-VPLS) over a multiprotocol label switching (MPLS) backbone. All interfaces attached to the VFI can participate in the switching. To delete the VFI, use the **no** form of this command.

l2 vfi *vfi-name* **manual**

no l2 vfi *vfi-name*

Syntax Description

vfi-name	Name assigned to the VFI.
manual	Specifies VFI manual configuration mode.

Defaults

No VFIs are created.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Entering the **l2 vfi** *vfi-name* **manual** command enables the VFI configuration mode. These configuration commands are available:

- **default**: sets the command to the default states.
- **exit**: exits VFI configuration mode and returns to global configuration mode.
- **no**: negates a command or set its defaults.
- **vpn id** *vpn-number*: specifies the virtual private network (VPN) ID of the VPLS configured by the VFI. For more information, see the **vpn id** command.

When you enter a **vpn id** *vpn-number,* these additional VFI configuration commands are available:

- **neighbor** *remote-peer-IP-address* **encapsulation mpls**: configures the IP address of the remote peer, which is to become a member of the VPLS configured by the VFI, and sets the MPLS encapsulation type.
- **shutdown**: shuts down the VFI interface.

The switch supports only one connection per VFI, so you can configure only one neighbor in a VFI. To complete the connection, you attach a VLAN or Ethernet interface to the VFI by using the **xconnect** interface configuration command. The switch supports multiple Ethernet interfaces or a single VLAN in a VFI. It does not support switching a VLAN and physical interfaces through the same VFI.

The switch supports a total of 26 VRFs and VPNs.

Note For more information about MPLS and VPLS, see the software configuration guide for this release.

Examples

This example shows how to configure a VLAN-based VPLS (*VFI abc*) between provider edge (PE) switch PE1's VLAN 3 interface and switch PE2's VLAN 4 interface. PE1 has IP address 10.0.0.1/32, and PE2 has IP address 20.0.011/32.

Enter these commands on the PE1 switch:

```
Switch(config)# l2 vfi abc manual
Switch(config-vfi)# vpn id 123
Switch(config-vfi)# neighbor 20.0.0.1 encapsulation mpls
Switch(config-vfi)# exit
Switch(config)# interface vlan 3
Switch(config-if)# xconnect vfi abc
```

Enter these commands on the PE2 switch:

```
Switch(config)# l2 vfi abc manual
Switch(config-vfi)# vpn id 123
Switch(config-vfi)# neighbor 10.0.0.1 encapsulation mpls
Switch(config-vfi)# exit
Switch(config)# interface vlan 4
Switch(config-if)# xconnect vfi abc
```

Related Commands

Command	Description
debug vfi	Displays VFI error or event debug messages.
show vfi	Displays detailed information about a VFI, including VFI parameters.
vpn id	Configures a VPN for the VFI VPLS.
xconnect	Attaches an interface to a VFI.

lacp port-priority

To configure the port priority for the Link Aggregation Control Protocol (LACP), use the **lacp port-priority** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

lacp port-priority *priority*

no lacp port-priority

Syntax Description

priority	Port priority for LACP. The range is 1 to 65535.

Defaults

The default is 32768.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **lacp port-priority** interface configuration command determines which ports are bundled and which ports are put in hot-standby mode when there are more than eight ports in an LACP channel group. This command takes effect only on EtherChannel ports that are already configured for LACP. If the interface is a user network interface (UNI), you must use the **port-type nni** or **port-type eni** interface configuration command to change the interface to an NNI or ENI before configuring **lacp port-priority**.

In priority comparisons, numerically *lower* values have *higher* priority. The switch uses the priority to decide which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from being active. If two or more ports have the same LACP port priority (for example, they are configured with the default setting of 65535), an internal value for the port number determines the priority.

Note The LACP port priorities are only effective if the ports are on the switch that controls the LACP link. See the **lacp system-priority** global configuration command for information about determining which switch controls the link.

Use the **show lacp internal** privileged EXEC command to display LACP port priorities and internal port number values.

For information about configuring LACP on physical ports, see the "Configuring EtherChannels" chapter in the software configuration guide for this release.

You can verify the configuration by entering the **show lacp** [*channel-group-number*] **internal** privileged EXEC command.

Examples

This example shows how to configure the LACP port priority on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# lacp port-priority 1000
```

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group.
lacp system-priority	Configures the LACP system priority.
show lacp [*channel-group-number*] **internal**	Displays internal information for all channel groups or for the specified channel group.

lacp system-priority

To configure the system priority for the Link Aggregation Control Protocol (LACP), use the **lacp system-priority** command in global configuration mode. To return to the default setting, use the **no** form of this command.

lacp system-priority *priority*

no lacp system-priority

Syntax Description

priority	System priority for LACP. The range is 1 to 65535.

Defaults

The default is 32768.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **lacp system-priority** command determines which switch in an LACP link controls port priorities. Although this is a global configuration command, the priority only takes effect on EtherChannels that have physical ports that are already configured for LACP.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. When there are more than eight ports in an LACP channel group, the switch on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other switch (the noncontrolling end of the link) are ignored.

In priority comparisons, numerically lower values have higher priority. Therefore, the switch with the numerically lower system value (higher priority value) for LACP system priority becomes the controlling switch. If both switches have the same LACP system priority (for example, they are both configured with the default setting of 32768), the LACP system ID (the switch MAC address) determines which switch is in control.

The **lacp system-priority** command applies to all LACP EtherChannels on the switch.

Use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag).

For more information about configuring LACP on physical ports, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

You can verify the configuration by entering the **show lacp sys-id** privileged EXEC command.

Examples

This example shows how to set the LACP system priority:

```
Switch(config)# lacp system-priority 20000
```

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group.
lacp port-priority	Configures the LACP port priority.
show lacp sys-id	Displays the system identifier that is being used by LACP.

location (global configuration)

To configure location information for a Link Layer Discovery Protocol (LLDP) endpoint, use the **location** command in global configuration mode. To remove the location information, use the **no** form of this command.

location {**admin-tag** ***string*** | **civic-location identifier** *id* | **elin-location** ***string*** **identifier** *id*}

no location {**admin-tag** ***string*** | **civic-location identifier** *id* | **elin-location** ***string*** **identifier** *id*}

Syntax Description

admin-tag	Configures administrative tag or site information.
civic-location	Configures civic location information.
elin-location	Configures emergency location information (ELIN).
identifier *id*	Specifies the ID for the civic location or the elin location. The ID range is 1 to 4095. **Note** The identifier for the civic location in the LLDP-MED TLV is limited to 250 bytes or less. To avoid error messages about available buffer space during switch configuration, be sure that the total length of all civic-location information specified for each civic-location identifier does not exceed 250 bytes.
string	Specifies the site or location information in alphanumeric format.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.(52)EY	This command was introduced.

Usage Guidelines

After entering the **location civic-location identifier** *id* global configuration command, you enter civic location configuration mode. In this mode, you can enter the civic location and the postal location information.

The civic-location identifier must not exceed 250 bytes.

Use the **no lldp med-tlv-select location** information interface configuration command to disable the location TLV. The location TLV is enabled by default. For more information, see the "Configuring LLDP and LLDP-MED" chapter of the software configuration guide for this release.

You can verify the configuration by entering the **show location elin** privileged EXEC command.

Examples

This example shows how to configure civic location information on the switch:

```
Switch(config)# location civic-location identifier 1
Switch(config-civic)# number 3550
Switch(config-civic)# primary-road-name "Cisco Way"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state CA
Switch(config-civic)# building 19
Switch(config-civic)# room C6
Switch(config-civic)# county "Santa Clara"
Switch(config-civic)# country US
Switch(config-civic)# end
```

This example shows how to configure the emergency location information location on the switch:

```
Switch (config)# location elin-location 14085553881 identifier 1
```

Related Commands

Command	Description
location (interface configuration)	Configures the location information for an interface.
show location	Displays the location information for an endpoint.

location (interface configuration)

To enter Link Layer Discovery Protocol (LLDP) location information for an interface, use the **location interface** command in interface configuration mode. To remove the interface location information, use the **no** form of this command.

location {**additional-location-information** *word* | **civic-location-id** *id* | **elin-location-id** *id*}

no location {**additional-location-information** *word* | **civic-location-id** *id* | **elin-location-id** *id*}

Syntax Description

additional-location-information	Configures additional information for a location or place.
word	Specifies
civic-location-id	Configures global civic location information for an interface.
elin-location-id	Configures emergency location information for an interface.
id	Specifies the ID for the civic location or the elin location. The ID range is 1 to 4095. **Note** The identifier for the civic location in the LLDP-MED TLV is limited to 250 bytes or less. To avoid error messages about available buffer space during switch configuration, be sure that the total length of all civic-location information specified for each civic-location identifier does not exceed 250 bytes.

Defaults

This command has no default setting.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

After entering the **location civic-location-id** *id* interface configuration command, you enter civic location configuration mode. In this mode, you can enter the additional location information.

The civic-location identifier must not exceed 250 bytes.

You can verify the configuration by entering the **show location elin interface** privileged EXEC command.

Examples

These examples show how to enter civic location information for an interface:

```
Switch(config-if)# int g1/0/1
Switch(config-if)# location civic-location-id 1
Switch(config-if)# end

Switch(config-if)# int g2/0/1
Switch(config-if)# location civic-location-id 1
Switch(config-if)# end
```

This example shows how to enter emergency location information for an interface:

```
Switch(config)# int g2/0/2
Switch(config-if)# location elin-location-id 1
Switch(config-if)# end
```

Related Commands

Command	Description
location (global configuration)	Configures the location information for an endpoint.
show location	Displays the location information for an endpoint.

logging event

To enable notification of interface link status changes, use the **logging event** command in interface configuration mode. To disable notification, use the **no** form of this command.

logging event {**bundle-status** | **link-status** | **spanning-tree** | **status** | **trunk status**}

no logging event {**bundle-status** | **link-status** | **spanning-tree** | **status** | **trunk status**}

Syntax Description

bundle-status	Enables notification of BUNDLE and UNBUNDLE messages.
link-status	Enables notification of interface data link status changes.
spanning-tree	Enables notification of spanning-tree events.
status	Enables notification of spanning-tree state change messages.
trunk-status	Enables notification of trunk-status messages.

Defaults

Event logging is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to enable spanning-tree logging:

```
Switch(config-if)# logging event spanning-tree
```

logging file

To set logging file parameters, use the **logging file** command in global configuration mode. To return to the default setting, use the **no** form of this command.

logging file *filesystem***:***filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*]

no logging file *filesystem***:***filename* [*severity-level-number* | *type*]

Syntax Description

filesystem:filename	Alias for a flash file system. Contains the path and name of the file that contains the log messages. The syntax for the local flash file system: **flash:**
max-file-size	(Optional) Specifies the maximum logging file size. The range is 4096 to 2147483647.
min-file-size	(Optional) Specifies the minimum logging file size. The range is 1024 to 2147483647.
severity-level-number	(Optional) Specifies the logging severity level. The range is 0 to 7. See the *type* option for the meaning of each level.
type	(Optional) Specifies the logging type. These keywords are valid: • **emergencies**—System is unusable (severity 0). • **alerts**—Immediate action needed (severity 1). • **critical**—Critical conditions (severity 2). • **errors**—Error conditions (severity 3). • **warnings**—Warning conditions (severity 4). • **notifications**—Normal but significant messages (severity 5). • **information**—Information messages (severity 6). • **debugging**—Debugging messages (severity 7).

Defaults

The minimum file size is 2048 bytes; the maximum file size is 4096 bytes.

The default severity level is 7 (**debugging** messages and numerically lower levels).

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The log file is stored in ASCII text format in an internal buffer on the switch. You can access logged system messages by using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. If the switch fails, the log is lost unless you had previously saved it to flash memory by using the **logging file flash:***filename* global configuration command.

After saving the log to flash memory by using the **logging file flash:***filename* global configuration command, you can use the **more flash:***filename* privileged EXEC command to display its contents.

The command rejects the minimum file size if it is greater than the maximum file size minus 1024; the minimum file size then becomes the maximum file size minus 1024.

Specifying a *level* causes messages at that level and numerically lower levels to be displayed.

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Examples

This example shows how to save informational log messages to a file in flash memory:

```
Switch(config)# logging file flash:logfile informational
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.

mac access-group

To apply a MAC access control list (ACL) to a Layer 2 interface, use the **mac access-group** command in interface configuration mode. To remove all MAC ACLs or the specified MAC ACL from the interface, use the **no** form of this command. You create the MAC ACL by using the **mac access-list extended** global configuration command.

mac access-group {*name*} **in**

no mac access-group {*name*}

Note You cannot attach an ACL to a Layer 2 port that has an Ethernet flow point (EFP) service instance configured on it. The **mac access-group** command is rejected on these ports.

Syntax Description

name	Specifies a named MAC access list.
in	Specifies that the ACL is applied in the ingress direction. Outbound ACLs are not supported on Layer 2 interfaces.

Defaults

No MAC ACL is applied to the interface.

Command Modes

Interface configuration (Layer 2 interfaces only)

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can apply MAC ACLs only to ingress Layer 2 interfaces. You cannot apply MAC ACLs to Layer 3 interfaces or to Layer 2 interfaces that have service instances configured on them.

On Layer 2 interfaces, you can filter IP traffic by using IP access lists and non-IP traffic by using MAC access lists. You can filter both IP and non-IP traffic on the same Layer 2 interface by applying both an IP ACL and a MAC ACL to the interface. You can apply no more than one IP access list and one MAC access list to the same Layer 2 interface.

If a MAC ACL is already configured on a Layer 2 interface and you apply a new MAC ACL to the interface, the new ACL replaces the previously configured one.

If you apply an ACL to a Layer 2 interface on a switch, and the switch has an input Layer 3 ACL or a VLAN map applied to a VLAN that the interface is a member of, the ACL applied to the Layer 2 interface takes precedence.

When an inbound packet is received on an interface with a MAC ACL applied, the switch checks the match conditions in the ACL. If the conditions are matched, the switch forwards or drops the packet, according to the ACL.

If the specified ACL does not exist, the switch forwards all packets.

You can verify MAC ACL configuration by entering the **show mac access-group** privileged EXEC command. You can see configured ACLs on the switch by entering the **show access-lists** privileged EXEC command.

Note For more information about configuring MAC extended ACLs, see the "Configuring Network Security with ACLs" chapter in the software configuration guide for this release.

Examples

This example shows how to apply a MAC extended ACL named *macacl2* to an interface:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mac access-group macacl2 in
```

Related Commands

Command	Description
show access-lists	Displays the ACLs configured on the switch.
show mac access-group	Displays the MAC ACLs configured on the switch.
show running-config	Displays the operating configuration.

mac access-list extended

To create an access list based on MAC addresses for non-IP traffic, use the **mac access-list extended** command in global configuration mode. Using this command puts you in the extended MAC access-list configuration mode. To return to the default setting, use the **no** form of this command.

Note You cannot apply named MAC extended ACLs to Layer 3 interfaces or to Layer 2 interfaces with service instances configured.

mac access-list extended *name*

no mac access-list extended *name*

Syntax Description

name	Assigns a name to the MAC extended access list.

Defaults

By default, there are no MAC access lists created.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

MAC named extended lists are used with VLAN maps and class maps.

You can apply named MAC extended ACLs to VLAN maps or to Layer 2 interfaces, except Layer 2 interfaces that have service instances configured on them.

You cannot apply named MAC extended ACLs to Layer 3 interfaces.

Entering the **mac access-list extended** command enables the MAC access-list configuration mode. These configuration commands are available:

- **default**: sets a command to its default.
- **deny**: specifies packets to reject. For more information, see the deny (MAC access-list configuration) MAC access-list configuration command.
- **exit**: exits from MAC access-list configuration mode.
- **no**: negates a command or sets its defaults.
- **permit**: specifies packets to forward. For more information, see the permit (MAC access-list configuration) command.

You can verify MAC ACL configuration by entering the **show access-lists** privileged EXEC command.

Note For more information about MAC extended access lists, see the software configuration guide for this release.

Examples

This example shows how to create a MAC named extended access list named *mac1* and to enter extended MAC access-list configuration mode:

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)#
```

This example shows how to delete MAC named extended access list *mac1*:

```
Switch(config)# no mac access-list extended mac1
```

Related Commands

Command	Description
deny (MAC access-list configuration) **permit** (MAC access-list configuration)	Configures the MAC ACL (in extended MAC-access list configuration mode).
show access-lists	Displays the access lists configured on the switch.
vlan access-map	Defines a VLAN map and enters access-map configuration mode where you can specify a MAC ACL to match and the action to be taken.

mac address-table aging-time

To set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated, use the **mac address-table aging-time** command in global configuration mode. To return to the default setting, use the **no** form of this command. The aging time applies to all VLANs or a specified VLAN.

mac address-table aging-time {**0** | *10-1000000*}[**bridge-domain** *domain-id* | **routed-mac** | **vlan** *vlan-id]*

no mac address-table aging-time {**0** | *10-1000000*} [**bridge-domain** *vlan-id* | **routed-mac** | **vlan** *vlan-id*]

Syntax Descriptionl

0	This value disables aging. Static address entries are never aged or removed from the table.
10-1000000	Aging time in seconds. The range is 10 to 1000000 seconds.
bridge-domain *domain-id*	(Optional) Specifies a bridge domain to which to apply the aging time. The bridge domain ID range is from 1 to 8000.
routed-mac	(Optional) Specifies applying the aging time to routed MAC addresses.
vlan *vlan-id*	(Optional) Specifies the VLAN ID to which to apply the aging time. The range is 1 to 4094.

Defaults

The default is 300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If hosts do not send continuously, increase the aging time to record the dynamic entries for a longer time. Increasing the time can reduce the possibility of flooding when the hosts send again.

If you do not specify a specific VLAN, this command sets the aging time for all VLANs and bridge domains.

You can verify your setting by entering the **show mac address-table aging-time** privileged EXEC command.

Examples

This example shows how to set the aging time to 200 seconds for all VLANs and bridge domains:

```
Switch(config)# mac address-table aging-time 200
```

Related Commands

Command	Description
show mac address-table aging-time	Displays the MAC address table aging time for all VLANs or the specified VLAN.

mac address-table learning

To enable MAC address learning on a VLAN or bridge domain, use the **mac address-table learning** command in global configuration mode. This is the default state. To disable MAC address learning to control which VLANs or bridge domains can learn MAC addresses, use the **no** form of this command.

mac address-table learning {**vlan** *vlan-id* | **bridge-domain** *domain-id*}

no mac address-table learning {**vlan** *vlan-id* | **bridge-domain** *domain-id*}

Syntax Description

bridge-domain *domain-id*	Specifies MAC address learning per bridge domain. The bridge domain ID range is from 1 to 8000.
vlan *vlan-id*	Specifies MAC address learning per VLAN. Valid VLAN IDs are 1 to 4094.

Defaults

By default, MAC address learning is enabled on all VLANs and bridge domains.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Customers in a service provider network can tunnel a large number of MAC addresses through the network and fill the available MAC address table space. When you control MAC address learning on a VLAN or bridge domain, you can manage the available MAC address table space by controlling which VLANs or bridge domains, and therefore which ports, can learn MAC addresses.

You can disable MAC address learning on a VLAN or bridge domain by entering the **no mac address-table learning** {**vlan** *vlan-id* | **bridge-domain** *domain-id*} command.

Before you disable MAC address learning, be sure that you are familiar with the network topology and the switch system configuration. Disabling MAC address learning could cause flooding in the network. For example, if you disable MAC address learning on a VLAN with a configured switch virtual interface (SVI), the switch floods all IP packets in the Layer 2 domain. If you disable MAC address learning on a VLAN that includes more than two ports, every packet entering the switch is flooded in that VLAN domain. We recommend that you disable MAC address learning only in VLANs that contain two ports and that you use caution before disabling MAC address learning on a VLAN with an SVI.

To display MAC address learning status or all VLANs and bridge domains, enter the **show mac-address-table learning** command. To display for a specific VLAN or bridge domain, enter the **show mac address-table learning** [**bridge-domain** *number*] [**vlan** *vlan-id*] command.

Examples

This example shows how to disable MAC address learning on VLAN 2003:

```
Switch(config)# no mac address-table learning vlan 2003
```

Related Commands

Command	Description
show mac address-table learning	Displays the MAC address learning status on all VLANs or on the specified VLAN.

mac address-table move update

To enable the MAC address-table move update feature, use the **mac address-table move update** command in global configuration mode. To return to the default setting, use the **no** form of this command.

mac address-table move update {**receive | transmit**}

no mac address-table move update {**receive | transmit**}

Syntax Description

receive	Specifies that the switch processes MAC address-table move update messages.
transmit	Specifies that the switch sends MAC address-table move update messages to other switches in the network if the primary link goes down and the standby link comes up.

Command Modes

Global configuration.

Defaults

By default, the MAC address-table move update feature is disabled.

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The MAC address-table move update feature allows the switch to provide rapid bidirectional convergence if a primary (forwarding) link goes down and the standby link begins forwarding traffic.

You can configure the access switch to send the MAC address-table move update messages if the primary link goes down and the standby link comes up. You can configure the uplink switches to receive and process the MAC address-table move update messages.

You can verify the configuration by entering the **show mac address-table move update** privileged EXEC command.

Examples

This example shows how to configure an access switch to send MAC address-table move update messages:

```
Switch# configure terminal
Switch(conf)# mac address-table move update transmit
Switch(conf)# end
```

This example shows how to configure an uplink switch to get and process MAC address-table move update messages:

```
Switch# configure terminal
Switch(conf)# mac address-table move update receive
Switch(conf)# end
```

Related Commands

Command	Description
clear mac address-table move update	Clears the MAC address-table move update global counters.
debug matm move	Debugs the MAC address-table move update message processing.
show mac address-table move update	Displays the MAC address-table move update information on the switch.

mac address-table notification

To enable the MAC address notification feature on the switch, use the **mac address-table notification** command in global configuration mode. To return to the default setting, use the **no** form of this command.

mac address-table notification {**change** [**history-size** *value* | **interval** *value*] | **mac-move** | **threshold** [[**limit** *percentage*] **interval** *time*]}

no mac address-table notification {**change** [**history-size** *value* | **interval** *value*] | **mac-move** | **threshold** [[**limit** *percentage*] **interval** *time*]}

Syntax Description

change	Enables or disables the MAC notification on the switch.
history-size *value*	(Optional) Configures the maximum number of entries in the MAC notification history table. The range is 1 to 500 entries. The default is 1.
interval *value*	(Optional) Sets the notification trap interval. The switch sends the notification traps when this amount of time has elapsed. The range is 0 to 2147483647 seconds. The default is 1 second.
mac-move	Enables MAC move notification.
threshold	Enable MACs threshold notification.
limit *percentage*	(Optional) Enters the MAC utilization threshold percentage. The range is 1 to 100 percent. The default is 50 percent.
interval *time*	(Optional) Enters the time between MAC threshold notifications. The range is 120 to 1000000 seconds. The default is 120 seconds.

Defaults

By default, the MAC address notification, MAC move, and MAC threshold monitoring are disabled.

The default MAC change trap interval is 1 second.

The default number of entries in the history table is 1.

The default MAC utilization threshold is 50 percent.

The default time between MAC threshold notifications is 120 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The MAC address notification change feature sends Simple Network Management Protocol (SNMP) traps to the network management system (NMS) whenever a new MAC address is added or an old address is deleted from the forwarding tables. MAC change notifications are generated only for dynamic and secure MAC addresses and are not generated for self addresses, multicast addresses, or other static addresses.

When you configure the **history-size** option, the existing MAC address history table is deleted, and a new table is created.

You enable the MAC address notification change feature by using the **mac address-table notification change** command. You must also enable MAC address notification traps on an interface by using the **snmp trap mac-notification change** interface configuration command and configure the switch to send MAC address traps to the NMS by using the **snmp-server enable traps mac-notification change** global configuration command.

You can also enable traps whenever a MAC address is moved from one port to another in the same VLAN by entering the **mac address-table notification mac-move** command and the **snmp-server enable traps mac-notification move** global configuration command.

To generate traps whenever the MAC address table threshold limit is reached or exceeded, enter the **mac address-table notification** *threshold* [**limit** *percentage*] | [**interval** *time*] command and the **snmp-server enable traps mac-notification threshold** global configuration command.

You can verify the configuration by entering the **show mac address-table notification** privileged EXEC command.

Examples

This example shows how to enable the MAC address-table change notification feature, set the interval time to 60 seconds, and set the history-size to 100 entries:

```
Switch(config)# mac address-table notification change
Switch(config)# mac address-table notification change interval 60
Switch(config)# mac address-table notification change history-size 100
```

Related Commands

Command	Description
clear mac address-table notification	Clears the MAC address notification global counters.
show mac address-table notification	Displays the MAC address notification settings on all interfaces or on the specified interface.
snmp-server enable traps	Sends the SNMP MAC notification traps when the **mac-notification** keyword is appended.
snmp trap mac-notification change	Enables the SNMP MAC notification trap on a specific interface.

mac address-table static

To add static addresses to the MAC address table or to enable unicast MAC address filtering, use the **mac address-table static** command in global configuration mode. To remove static entries from the table or return to the default setting, use the **no** form of this command.

mac address-table static *mac-addr* **vlan** *vlan-id* {**drop | interface** *interface-id*}

no mac address-table static *mac-addr* **vlan** *vlan-id* [drop | **interface** *interface-id*]

Syntax Description

mac-addr	Destination MAC address (unicast or multicast) to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface.
vlan *vlan-id*	Specifies the VLAN for which the packet with the specified MAC address is received. The range is 1 to 4094.
drop	Configures the switch to drop traffic with a specific source or destination MAC address.
interface *interface-id*	Interface to which the received packet is forwarded. Valid interfaces include physical ports and port channels.

Defaults

No static addresses are configured.

Unicast MAC address filtering is disabled. The switch does not drop traffic for specific source or destination MAC addresses.

Command Modes

Global configuration

Command History

Release	Modification
12.2(452)EY	This command was introduced.

Usage Guidelines

Follow these guidelines when using the **drop** keyword to configure MAC address filtering:

- Multicast MAC addresses, broadcast MAC addresses, and router MAC addresses are not supported. Packets that are forwarded to the CPU are also not supported.
- If you add a unicast MAC address as a static address and configure unicast MAC address filtering, the switch either adds the MAC address as a static address or drops packets with that MAC address, depending on which command was entered last. The second command that you entered overrides the first command.

  For example, if you enter the **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* global configuration command followed by the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** command, the switch drops packets with the specified MAC address as a source or destination.

If you enter the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** global configuration command followed by the **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* command, the switch adds the MAC address as a static address.

You can verify your setting by entering the **show mac address-table** or **show mac address-table static** privileged EXEC command.

Examples

This example shows how to enable unicast MAC address filtering and to configure the switch to drop packets that have a source or destination address of c2f3.220a.12f4. When a packet is received in VLAN 4 with this MAC address as its source or destination, the packet is dropped:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

This example shows how to disable unicast MAC address filtering:

```
Switch(config)# no mac address-table static c2f3.220a.12f4 vlan 4
```

This example shows how to add the static address c2f3.220a.12f4 to the MAC address table. When a packet is received in VLAN 4 with this MAC address as its destination, the packet is forwarded to the specified interface:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet0/1
```

Related Commands

Command	Description
show mac address-table static	Displays static MAC address table entries only.

macro apply

To apply a macro to an interface or to apply and trace a macro configuration on an interface, use the **macro apply** or **macro trace** command in interface configuration command.

macro {**apply** | **trace**} *macro-name* [*parameter value*] [*parameter value*] [*parameter value*]

Note There is not a **no** form of this command.

Syntax Description

apply	Applies a macro to the specified interface.
trace	Uses the **trace** keyword to apply a macro to an interface and to debug the macro.
macro-name	Specifies the name of the macro.
parameter value	(Optional) Specifies unique parameter values that are specific to the interface. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value.

Defaults

This command has no default setting.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can use the **macro trace** *macro-name* interface configuration command to apply and show the macros running on an interface or to debug the macro to find any syntax or configuration errors.

If a command fails because of a syntax error or a configuration error when you apply a macro, the macro continues to apply the remaining commands to the interface.

When creating a macro that requires the assignment of unique values, use the *parameter value* keywords to designate values specific to the interface.

Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a larger string, is considered a match and is replaced by the corresponding value.

Some macros might contain keywords that require a parameter value. You can use the **macro apply** *macro-name* **?** command to display a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied.

When you apply a macro to an interface, the macro name is automatically added to the interface. You can display the applied commands and macro names by using the **show running-configuration interface** *interface-id* user EXEC command.

A macro applied to an interface range behaves the same way as a macro applied to a single interface. When you use an interface range, the macro is applied sequentially to each interface within the range. If a macro command fails on one interface, it is still applied to the remaining interfaces.

You can delete a macro-applied configuration on an interface by entering the **default interface** *interface-id* interface configuration command.

Examples

After you have created a macro by using the **macro name** global configuration command, you can apply it to an interface. This example shows how to apply a user-created macro called **duplex** to an interface:

```
Switch(config-if)# macro apply duplex
```

To debug a macro, use the **macro trace** interface configuration command to find any syntax or configuration errors in the macro as it is applied to an interface. This example shows how troubleshoot the user-created macro called **duplex** on an interface:

```
Switch(config-if)# macro trace duplex
Applying command...'duplex auto'
%Error Unknown error.
Applying command...'speed nonegotiate'
```

Related Commands

Command	Description
macro description	Adds a description about the macros that are applied to an interface.
macro global	Applies a macro on a switch or applies and traces a macro on a switch.
macro global description	Adds a description about the macros that are applied to the switch.
show parser macro	Displays the macro definition for all macros or for the specified macro.

macro description

To enter a description about which macros are applied to an interface, use the **macro description** command in interface configuration mode. To remove the description, use the **no** form of this command.

macro description *text*

no macro description *text*

Syntax Description

description *text*	Enters a description about the macros that are applied to the specified interface.

Defaults

This command has no default setting.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use the **description** keyword to associate comment text, or the macro name, with an interface. When multiple macros are applied on a single interface, the description text will be from the last applied macro.

This example shows how to add a description to an interface:

```
Switch(config-if)# macro description duplex settings
```

You can verify your settings by entering the **show parser macro description** privileged EXEC command.

Related Commands

Command	Description
macro apply	Applies a macro on an interface or applies and traces a macro on an interface.
macro global	Applies a macro on a switch or applies and traces a macro on a switch
macro global description	Adds a description about the macros that are applied to the switch.
show parser macro	Displays the macro definition for all macros or for the specified macro.

macro global

To apply a macro to a switch or to apply and trace a macro configuration on a switch, use the **macro global** command in global configuration mode.

macro global {**apply** | **trace**} *macro-namemacro-name* [*parameter value*] [*parameter value*] [*parameter value*]

Syntax Description

apply	Applies a macro to the switch.
trace	Applies a macro to a switch and to debug the macro.
macro-name	Specifies the name of the macro.
parameter value	(Optional) Specifies unique parameter values that are specific to the switch. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can use the **macro trace** *macro-name* global configuration command to apply and to show the macros running on a switch or to debug the macro to find any syntax or configuration errors.

If a command fails because of a syntax error or a configuration error when you apply a macro, the macro continues to apply the remaining commands to the switch.

When creating a macro that requires the assignment of unique values, use the **parameter** *value* keywords to designate values specific to the switch.

Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a larger string, is considered a match and is replaced by the corresponding value.

Some macros might contain keywords that require a parameter value. You can use the **macro global apply** *macro-name* **?** command to display a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied.

When you apply a macro to a switch, the macro name is automatically added to the switch. You can display the applied commands and macro names by using the **show running-configuration** user EXEC command.

You can delete a global macro-applied configuration on a switch only by entering the **no** version of each command contained in the macro.

Examples

After you have created a new macro by using the **macro name** global configuration command, you can apply it to a switch. This example shows how see the **snmp** macro and how to apply the macro and set the hostname to test-server and set the IP precedence value to 7:

```
Switch# show parser macro name snmp
Macro name : snmp
Macro type : customizable

#enable port security, linkup, and linkdown traps
snmp-server enable traps port-security
snmp-server enable traps linkup
snmp-server enable traps linkdown
#set snmp-server host
snmp-server host ADDRESS
#set SNMP trap notifications precedence
snmp-server ip precedence VALUE

------------------------------------------------
Switch(config)# macro global apply snmp ADDRESS test-server VALUE 7
```

To debug a macro, use the **macro global trace** global configuration command to find any syntax or configuration errors in the macro when it is applied to a switch. In this example, the **ADDRESS** parameter value was not entered, causing the `snmp-server host` command to fail while the remainder of the macro is applied to the switch:

```
Switch(config)# macro global trace snmp VALUE 7
Applying command...'snmp-server enable traps port-security'
Applying command...'snmp-server enable traps linkup'
Applying command...'snmp-server enable traps linkdown'
Applying command...'snmp-server host'
%Error Unknown error.
Applying command...'snmp-server ip precedence 7'
```

Related Commands

Command	Description
macro apply	Applies a macro on an interface or applies and traces a macro on an interface.
macro description	Adds a description about the macros that are applied to an interface.
macro global description	Adds a description about the macros that are applied to the switch.
show parser macro	Displays the macro definition for all macros or for the specified macro.

macro global description

To enter a description about the macros that are applied to the switch, use the **macro global description** in global configuration mode. To remove the description, use the **no** form of this command

macro global description *text*

no macro global description *text*

Syntax Description

description *text*	A description of the macros that are applied to the switch.

Defaults

This command has no default setting.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use the **description** keyword to associate comment text, or the macro name, with a switch. When multiple macros are applied on a switch, the description text will be from the last applied macro.

This example shows how to add a description to a switch:

```
Switch(config)# macro global description udld aggressive mode enabled
```

You can verify your settings by entering the **show parser macro description** privileged EXEC command.

Related Commands

Command	Description
macro apply	Applies a macro on an interface or applies and traces a macro on an interface.
macro description	Adds a description about the macros that are applied to an interface.
macro global	Applies a macro on a switch or applies and traces a macro on a switch.
show parser macro	Displays the macro definition for all macros or for the specified macro.

match (access-map configuration)

To match packets against one or more access lists, use the **match** command in access-map configuration command mode to set the VLAN map. To remove the match parameters, use the **no** form of this command.

match {**ip address** {*name* | *number*} [*name* | *number*] [*name* | *number*]...} | {**mac address** {*name*} [*name*] [*name*]...}

no match {**ip address** {*name* | *number*} [*name* | *number*] [*name* | *number*]...} | {**mac address** {*name*} [*name*] [*name*]...}

Syntax Description

ip address	Sets the access map to match packets against an IP address access list.
mac address	Sets the access map to match packets against a MAC address access list.
name	Name of the access list to match packets against.
number	Number of the access list to match packets against. This option is not valid for MAC access lists.

Defaults

The default action is to have no match parameters applied to a VLAN map.

Command Modes

Access-map configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

In access-map configuration mode, use the **match** command to define the match conditions for a VLAN map applied to a VLAN. Use the **action** command to set the action that occurs when the packet matches the conditions.

Packets are matched only against access lists of the same protocol type; IP packets are matched against IP access lists, and all other packets are matched against MAC access lists.

Both IP and MAC addresses can be specified for the same map entry.

You can verify the configuration by entering the **show vlan access-map** privileged EXEC command.

Examples

This example shows how to define and apply a VLAN access map *vmap4* to VLANs 5 and 6 that will cause the interface to drop an IP packet if the packet matches the conditions defined in access list *al2*.

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan filter vmap4 vlan-list 5-6
```

Related Commands

Command	Description
access-list	Configures a standard numbered ACL. For syntax information, select **Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands**.
action	Specifies the action to be taken if the packet matches an entry in an access control list (ACL).
ip access list	Creates a named access list. For syntax information, select **Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands**.
mac access-list extended	Creates a named MAC address access list.
show vlan access-map	Displays the VLAN access maps created on the switch.
vlan access-map	Creates a VLAN access map.

match access-group

To configure the match criteria for a class map on the basis of the specified access control list (ACL), use the **match access-group** command in class-map configuration mode. To remove the ACL match criteria, use the **no** form of this command.

match access-group *acl-index-or-name*

no match access-group *acl-index-or-name*

Syntax Description

acl-index-or-name	Number or name of an IP standard or extended access control list (ACL) or MAC ACL. The range is from 1 to 2799. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.

Defaults

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **match access-group** command specifies a numbered or named ACL to use as the match criteria to determine if packets belong to the class specified by the class map.

Before using the **match access-group** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

You can use the **match access-group** classification only on input policy maps.

You can verify the configuration by entering the **show class-map** privileged EXEC command.

Examples

This example shows how to create a class map called in*class*, which uses the access control list *acl1* as the match criterion:

```
Switch(config)# class-map match-any inclass
Switch(config-cmap)# match access-group acl1
Switch(config-cmap)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
show class-map	Displays quality of service (QoS) class maps.

match cos

To match a packet based on a Layer 2 class of service (CoS) marking, use the **match cos** command in class-map configuration mode. You can match on the outer VLAN tag or the inner (customer) tag). to remove the CoS match criteria, use the **no** form of this command.

match cos {*cos-list* | **inner** *cos-list*}

no match cos {*cos-list* | **inner** *cos-list*}

Syntax Description

cos *cos-list*	Matches a packet based on the outer VLAN tag or the service-provider CoS value (S-CoS). You can specify up to four CoS values to match against incoming packets. Separate each value with a space. The range is 0 to 7.
cos inner *cos-list*	Matches a packet based on the C-CoS, the inner (customer) CoS value of an 802.1Q tunnel. For packets with less than two tags, this command has no effect. You can specify up to four CoS values to match against incoming packets. Separate each value with a space. The range is 0 to 7.

Defaults

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **match cos** and **match cos inner** commands specify a CoS value to use as the match criteria to determine if packets belong to the class specified by the class map.

Before using the **match cos** or **match cos inner command**, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

Matching of CoS values is supported only on ports carrying Layer 2 VLAN-tagged traffic. That is, you can use the **cos** classification only on IEEE 802.1Q trunk ports.

You can use **match cos** and **match cos inner** classification in input and output policy maps.

You can verify the configuration by entering the **show class-map** privileged EXEC command.

Examples

This example shows how to create a class map called in*class*, which matches all the incoming traffic with CoS values of 1 and 4:

```
Switch(config)# class-map match-any in-class
Switch(config-cmap)# match cos 1 4
Switch(config-cmap)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
show class-map	Displays quality of service (QoS) class maps.

match discard-class

To configure the match criteria for a class map based on the drop precedence of a packet during congestion management, use the **match discard-class** command in class-map configuration mode. To remove the match criteria, use the **no** form of this command.

match discard-class *value*

no match discard-class *value*

Syntax Description

value	Sets a drop precedence for a packet during congestion management. The range is from 0 to 7. Matching discard is supported only in output policy maps.

Defaults

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **match discard-class** command specifies a drop value to use as the match criteria to determine if packets belong to the class specified by the class map.

Before using the **match discard-class** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

You can use the **match discard-class** classification only on output policy maps.

You can verify the configuration by entering the **show class-map** privileged EXEC command.

Examples

This example shows how to create a class map called *outclass*, which uses a drop value of 5 as the match criterion:

```
Switch(config)# class-map match-any outclass
Switch(config-cmap)# match discard-class 5
Switch(config-cmap)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
show class-map	Displays quality of service (QoS) class maps.

match ip dscp

To identify a specific IPv4 Differentiated Service Code Point (DSCP) value as match criteria for a class, use the **match ip dscp** command inclass-map configuration mode. To remove the match criteria, use the **no** form of this command.

match ip dscp *dscp-list*

no match ip dscp *dscp-list*

Syntax Description

ip-dscp-list	List of up to eight IPv4 DSCP values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You can also enter a mnemonic name for a commonly used value and configure DSCP values in other forms (af numbers, cs numbers, **default**, or **ef**). See the "Configuring QoS" chapter in the software configuration guide for this release for information about other options for specifying DSCP values.

Defaults

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **match ip dscp** command specifies a DSCP value to use as the match criteria to determine if packets belong to the class specified by the class map.

This command is used by the class map to identify a specific DSCP value marking on a packet. In this context, DSCP values are used as markings only and have no mathematical significance. For example, the DSCP value of 2 is not greater than 1, but merely indicates that a packet marked with a value of 2 is different than one marked with a value of 1. You define the treatment of these marked packets by setting QoS policies in policy-map class configuration mode.

Before using the **match ip dscp** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

You can enter up to eight DSCP values in one match statement. For example, if you wanted the DCSP values of 0, 1, 2, 3, 4, 5, 6, or 7, enter the **match ip dscp 0 1 2 3 4 5 6 7** command. The packet must match only one (not all) of the specified IPv4 DSCP values to belong to the class.

You can use **match ip dscp** classification in input and output policy maps.

You can verify the configuration by entering the **show class-map** privileged EXEC command.

Examples

This example shows how to create a class map called in*class*, which matches all the incoming traffic with DSCP values of 10, 11, and 12:

```
Switch(config)# class-map match-any in-class
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
show class-map	Displays quality of service (QoS) class maps.

match ip precedence

To identify IPv4 precedence values as match criteria for a class, use the **match ip precedence** command in class-map configuration mode. To remove the match criteria, use the **no** form of this command.

match ip precedence *ip-precedence-list*

no match ip precedence *ip-precedence-list*

Syntax Description

ip precedence *ip-precedence-list*	List of up to four IPv4 precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. You enter these keywords for precedence: • **0** to **7**—Enter up to 4 precedence values separated by spaces. • **critical**—Match packets with critical precedence (5). • **flash**—Match packets with flash precedence (3). • **flash-override**—Match packets with flash override precedence (4). • **immediate**—Match packets with immediate precedence (2). • **internet**—Match packets with internetwork control precedence (6). • **network**—Match packets with network control precedence (7). • **priority**—Match packets with priority precedence (1). • **routine**—Match packets with routine precedence (0).

Defaults

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **match ip precedence** command specifies an IPv4 precedence value to use as the match criteria to determine if packets belong to the class specified by the class map.

The precedence values are used as marking only. In this context, the IP precedence values have no mathematical significance. For example, the precedence value of 2 is not greater than 1, but merely indicates that a packet marked with a value of 2 is different than one marked with a value of 1. You define the treatment of these marked packets by setting QoS policies in policy-map class configuration mode.

Before using the **match ip precedence** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

You can enter up to four IPv4 precedence values in one match statement. For example, if you wanted the IP precedence values of 0, 1, 2, or 7, enter the **match ip precedence 0 1 2 7** command. The packet must match only one (not all) of the specified IP precedence values to belong to the class.

You can use **match ip precedence** classification in input and output policy maps.

You can verify the configuration by entering the **show class-map** privileged EXEC command.

Examples

This example shows how to create a class map called *class*, which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:

```
Switch(config)# class-map match-any in-class
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
show class-map	Displays quality of service (QoS) class maps.

match mpls experimental topmost

To identify the outer multiprotocol label switching (MPLS) experimental label to use as the match criteria for a class, use the **mpls experimental topmost** command in class-map configuration mode. To remove the match criteria, use the **no** form of this command.

match experimental topmost *value*

no match experimental topmost *value*

Syntax Description

value	A list of up to eight MPLS experimental labels. You can enter multiple lines to match more than eight MPLS experimental values. This keyword matches only valid MPLS packets. Separate each value with a space. The range is 0 to 7.

Defaults

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **match experimental topmost** *value* command specifies a value for the topmost (outer) MPLS label to use as the match criteria to determine if packets belong to the class specified by the class map.

Before using the **match experimental topmost** *value* command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

You can enter up to eight MPLS EXP label values in one match statement. You can enter multiple lines to match more than eight values.

In an MPLS network, the IP precedence bits in the packet header are copied into the MPLS EXP fields at the edge of a network. Instead of overwriting the value in the IP precedence field, you can set the MPLS experimental bit. You can use different values to mark packets based on characteristics such as rate or type so that packets have the same priority.

You can use **match experimental topmost** *value* classification in input and output policy maps.

You can verify the configuration by entering the **show class-map** privileged EXEC command.

Examples

This example shows how to create a class map called in*class*, which matches all the incoming traffic with MPLS values of 5 and 6:

```
Switch(config)# class-map match-any in-class
Switch(config-cmap)# match mpls experimental topmost 5 6
Switch(config-cmap)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
show class-map	Displays quality of service (QoS) class maps.

match qos-group

To identify a specific quality of service (QoS) group value as a match criterion for a class, use the **match qos-group** command in class-map configuration mode. To remove the match criteria, use the **no** form of this command.

match qos-group *value*

no match qos-group *value*

Syntax Description

qos-group *value*	A quality of service group value. The range is from 0 to 99.

Defaults

No match criterion are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **match qos-group** command specifies a QoS group value to use as the match criterion to determine if packets belong to the class specified by the class map.

The QoS-group values are used as marking only and have no mathematical significance. For example, the precedence value of 2 is not greater than 1, but merely indicates that a packet marked with a value of 2 is different than one marked with a value of 1. You define the treatment of these marked packets by setting QoS policies in policy-map class configuration mode.

The QoS-group value is local to the switch, meaning that the QoS-group value marked on a packet does not leave the switch when the packet leaves the switch. If you require a marking that remains with the packet, use IP Differentiated Service Code Point (DSCP) values, IP precedence values, or another method of packet marking.

Before using the **match qos-group** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

You can use the **match qos-group** classification only on output policy maps.

There can be no more than 100 QoS groups on the switch (0 to 99).

You can verify the configuration by entering the **show class-map** privileged EXEC command.

Examples

This example shows how to classify traffic by using QoS group 13 as the match criterion:

```
Switch(config)# class-map match-any inclass
Switch(config-cmap)# match qos-group 13
Switch(config-cmap)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
show class-map	Displays QoS class maps.

match vlan

To apply QoS policies to frames carried on a user-specified VLAN for a given interface, use the **match vlan** command in class-map configuration mode in the parent policy of a hierarchical policy map. You can use hierarchical policy maps for per-VLAN classification on trunk ports. To remove the match criteria, use the **no** form of this command.

match vlan {*vlan-list* | **inner** *vlan-list*}

no match vlan {*vlan-list* | **inner** *vlan-list*}

Syntax Description

vlan *vlan-list*	Specifies matching a packet based on the outermost, service-provider VLAN ID (S-VLAN). For untagged packets, this matches the default VLAN associated with the packets from the port or EFP. You can enter a single VLAN ID or a range of VLANs separated by a hyphen. The range is from 1 to 4094.
vlan inner *vlan-list*	Specifies matching a packet based on the C-VLAN, the inner customer VLAN ID of an 802.1Q tunnel. For packets with less than 2 tags, the command has no effect. You can specify a single VLAN identified by a VLAN number or a range of VLANs separated by a hyphen. The range is 1 to 4094.

Defaults

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You configure per-VLAN QoS by entering the **match vlan** *vlan-id* or **match vlan-inner** *vlan-id* class-map configuration command for one or more VLANs.

The feature is supported using a 2-level hierarchical input policy map, where the parent-level defines the VLAN-based classification, and the child-level defines the QoS policy to be applied to the corresponding VLAN(s).

You use the **match vlan** *vlan-id* class-map configuration command to classify based on the outer VLAN. Use the **match vlan inner** *vlan-id* class-map configuration command to classify based on the inner VLAN

With classification based on VLAN IDs, you can apply QoS policies to frames carried on a user-specified VLAN for a given interface. You can use hierarchical policy maps for per-VLAN classification on trunk ports. Per-VLAN classification is not required on access ports because access ports carry traffic for a single VLAN.

Per-port, per-VLAN QoS is supported only on IEEE 802.1Q trunk ports.

Before using the **match vlan** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

You can verify your configuration by entering the **show class-map** privileged EXEC command.

Examples

This example shows how to create a class-map called *parent-class*, which matches incoming traffic with VLAN IDs in the range from 30 to 40.

```
Switch(config)# class-map match-any parent-class
Switch(config-cmap)# match vlan 30-40
Switch(config-cmap)# exit
```

This example shows how to match VLAN and CoS in the same policy. When you attach the service policy *vlan* to an interface, packets with the outer VLAN of 2 and an outer CoS of 2 are included in class map *phb*.

```
Switch(config)# class-map vlan
Switch(config-cmap)# match vlan 2
Switch(config-cmap)# exit
Switch(config)# class-map phb
Switch(config-cmap)# match cos 2
Switch(config-cmap)# exit
Switch(config)# policy-map phb
Switch(config-pmap)# class phb
Switch(config-pmap-c)# bandwidth 1000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map vlan
Switch(config-pmap)# class vlan
Switch(config-pmap-c)# bandwidth 1000
Switch(config-pmap-c)# service-policy phb
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy vlan
Switch(config-if)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class name.
show class-map	Displays quality of service (QoS) class maps.

max-delay

To configure the maximum length of time a Maintenance Endpoint (MEP) in an IP Service Level Agreements (SLAs) Metro-Ethernet 3.0 (ITU-T Y.1731) operation waits for a synthetic frame, use the max-delay command in IP SLA Y1731 delay configuration mode. To return to the default, use the no form of this command.

max-delay *milliseconds*

no max-delay

Syntax Description

milliseconds	Maximum delay in milliseconds (ms). The range is from 1 to 65535. The default is 5000

Defaults

The default for max-delay is 5000 milliseconds.

Command Modes

IP SLA Y.1731 delay configuration (config-sla-y1731-delay)

Command History

Release	Modification
12.2(4)S1	This command was introduced.

Usage Guidelines

Use this command to change the maximum amount of time an MEP in an Ethernet delay or delay variation operation will wait for a synthetic frame from the default (5000 ms) to the specified value.

Examples

This example shows how to enable auto-MDIX on a port:

```
Switch(config-term)# ip sla 501
Switch(config-ip-sla)# ethernet y1731 delay receive 1DM domain xxx evc yyy cos 3 mpid 101
Switch(config-sla-y1731-delay)#max-delay 2000

Switch # show ip sla configuration 501
IP SLAs Infrastructure Engine-III
Entry number: 501
Owner: admin
Tag:
Operation timeout (milliseconds): 5000
Ethernet Y1731 Delay Operation
Frame Type: 1DM
Domain: xxx
ReceiveOnly: TRUE
Evc: yyy
Local Mpid: 101
CoS: 3
   Max Delay: 5000
Threshold (milliseconds): 2000
.
.
```

```
.
Statistics Parameters
  Aggregation Period: 900
  Frame offset: 1
  Distribution Delay One-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
  Distribution Delay-Variation One-Way:
   Number of Bins 10
   Bin Boundaries: 5000,10000,15000,20000,25000,30000,35000,40000,45000,-1
History
  Number of intervals: 2
```

Related Commands

Command	Description
show controllers ethernet-controller *interface-id* **phy**	Displays general information about internal registers of an interface, including the operational state of auto-MDIX.

mdix auto

To enable the automatic medium-dependent interface crossover (auto-MDIX) feature on the interface, use the **mdix auto** command in interface configuration mode. When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately. To disable auto-MDIX, use the **no** form of this command.

mdix auto

no mdix auto

Syntax Description

This command has no arguments or keywords.

Defaults

Auto-MDIX is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When you enable auto-MDIX on an interface, you must also set the speed and duplex on the interface to **auto** so that the feature operates correctly.

When auto-MDIX (along with autonegotiation of speed and duplex) is enabled on one or both of connected interfaces, link up occurs, even if the required cable type (straight-through or crossover) is not present.

Auto-MDIX is supported on all 10/100-Mbps interfaces and on 10/100/1000BASE-T/BASE-TX small form-factor pluggable (SFP)-module interfaces. It is not supported on 1000BASE-SX or -LX SFP module interfaces.

You can verify the operational state of auto-MDIX on the interface by entering the **show controllers ethernet-controller** *interface-id* **phy** privileged EXEC command.

Examples

This example shows how to enable auto-MDIX on a port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

Related Commands

Command	Description
show controllers ethernet-controller *interface-id* **phy**	Displays general information about internal registers of an interface, including the operational state of auto-MDIX.

mtu

To set the maximum packet size or maximum transmission unit (MTU) size for an interface, use the **mtu** command in interface configuration mode. To return to the default value, use the **no** form of this command.

mtu *bytes*

no mtu *bytes*

Syntax Description

bytes	Set the system MTU for the interface. The range is from 1500 to 9800 bytes. The default is 1500.

Defaults

The default maximum transmission unit (MTU) size for frames received and sent on all interfaces on the switch is 1500 bytes.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When you use this command to change the MTU size on an interface, it is not necessary to reset the switch before the new configuration takes effect.

Because the switch does not fragment Layer 2 packets, it drops switched Layer 2 packets larger than the packet size supported on the *egress* interface.

Examples

This example shows how to set the maximum packet size for a port to 1800 bytes:

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# mtu 1800
Switch(config)# exit
```

Related Commands

Command	Description
show interface [*interface-id*] **mtu**	Displays the MTU size for all interfaces or for the specified interface.

network-clock hold-off

To configure the time that the switch waits when a SyncE reference clock goes down before removing it as the network clock, use the **network-clock hold-off** command in global configuration mode. To return to the default value, use the no form of this command.

network-clock hold-off *value*

no network-clock hold-off *value*

Syntax Description

value	Sets the time in milliseconds. The accepted values are: • 50 to 10000 milliseconds (ms) – The timeout value. The default is 300 ms. • 0 = Hold-off disable

Defaults

The default hold-off time is 300 ms.

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)EY	This command was introduced.

Usage Guidelines

Setting a hold-off timeout ensures that the short activation of a signal failure is not passed to the clock selection process.

Examples

The following example shows how to set the hold-off time.

```
Switch# config t
Switch(config)# network-clock hold-off 1000
```

Related Commands

Command	Description
show network-clocks	Displays network clock configuration.
show network-clock synchronization	Displays network clock configuration.
controller BITS commands	Configures the BITS clock controller characteristics.

network-clock input-source

To configure the Synchronous Ethernet (SyncE) input clock and priority, use the **network-clock input-source** command in global configuration mode. To remove the priority, use the no form of this command.

network-clock input-source *priority* [**external] [interface]**

no network-clock input-source *priority* [**external] [interface]**

Syntax Description

priority	Sets the priority of the device as a network clock. The range is from 1 to 250, with 1 being the highest priority. Unused network clocks are given a priority value of 0.
external	Specifies the type of external interface: • BITS • SSU • GPS
interface	Specifies the type of interface: • Ethernet • Sonet • ToP

Defaults

The SyncE network clock is not configured.

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)EY	This command was introduced.

Usage Guidelines

During operation, the system selects the network clock based on the priority.

Examples

Example 1 - SYNCE as Clock Source

The following example shows how to configure SyncE as the network clock input source.

```
Switch(config)# network-clock input-source 1 interface tenGigabitEthernet ?
<0-0> TenGigabitEthernet interface number
```

Example 2 - BITS as Clock Source

The following example shows how to configure BITS as the network clock input source.

```
Switch(config)# network-clock input-source 1 external 1/0/0 e1 ?
cas   E1 Channel Associated Signal Mode
crc4  E1 With CRC4 Signal Mode
fas   E1 Frame Alignment Signal Mode
```

Related Commands

Command	Description
show network-clocks	Displays network clock configuration.
show network-clock synchronization	Displays network clock configuration.
controller BITS commands	Configures the BITS clock controller characteristics.

network-clock revertive

To configure the Synchronous Ethernet (SyncE) input clock to determine the action to take if clock reference with higher priority than the selected reference clock becomes available, use the network-clock revertive command in global configuration mode. To return to the default value, use the no form of this command.

network-clock revertive

no network-clock revertive

Syntax Description

This command has no arguments or keywords.

Defaults

The default is non-revertive.

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)EY	This command was introduced.

Usage Guidelines

The network clock can be selected by an automatic selection algorithm based on the highest priority valid input clock. In revertive mode, the network clock is automatically selected reference based on the configured priority of the clock.

Examples

The following example shows how to configure the network-clock as revertive.

```
Switch# config t
Switch(config)# network-clock revertive
```

Related Commands

Command	Description
show network-clocks	Displays network clock configuration.
show network-clock synchronization	Displays network clock configuration.
controller BITS commands	Configures the BITS clock controller characteristics.

network-clock synchronization ssm option

To configure the Synchronous Status Message (SSM) option for a Synchronous Ethernet (SynchE) network clock, use the **network-clock synchronization ssm option** command in global configuration mode. To return to the default value, use the no form of this command.

network-clock synchronization ssm option [[**1** | **2**] **GEN1** | **GEN2**]

no network-clock synchronization ssm option [[**1** | **2**] **GEN1** | **GEN2**]

Syntax Description

1	Synchronization networking Option I
2	Synchronization networking Option II
GEN1	Option II Generation 1
GEN2	Option II Generation 2

Defaults

The default is Option 1.

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)EY	This command was introduced.

Usage Guidelines

When Option 2 is selected, GEN1 must be configured. GEN2 is not supported in Release 15.1(2)EY.

Examples

The following example shows how to configure the ssm option:

```
Switch# config t
Switch(config)# network-clock synchronization ssm option 2 GEN1
```

Related Commands

Command	Description
show network-clocks	Displays network clock configuration.
show network-clock synchronization	Displays network clock configuration.
controller BITS commands	Configures the BITS clock controller characteristics.

network-clock wait-to-restore

To configure the time that the switch waits before a previously failed Synchronous Ethernet (SyncE) input clock must be fault-free before it is considered available as a synchronization source, use the **network-clock wait-to-restore** command in global configuration mode. To return to the default value, use the no form of this command.

network-clock wait-to-restore *value*

no network-clock wait-to-restore *value*

Syntax Description

value	Sets the wait time in seconds. The range is 0 to 86400 seconds. The default is 300 seconds.

Defaults

SyncE wait to restore time is 300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)EY	This command was introduced.

Usage Guidelines

Examples

The following example shows how to configure the wait-to-restore time:

```
Switch# config t
Switch(config)# network-clock wait-to-restore 50000
```

Related Commands

Command	Description
show network-clocks	Displays network clock configuration.
show network-clock synchronization	Displays network clock configuration.
controller BITS commands	Configures the BITS clock controller characteristics.

network-clock-select

To configure the Synchronous Ethernet (SyncE) input clock and priority, use the **network-clock-select** command in global configuration mode. To remove the priority, use the **no** form of this command.

network-clock-select *priority* [**BITS** | **SYNCE** *port-number*]

no network-clock-select *priority*

Syntax Description

priority	Sets the priority of the device as a network clock. The range is from 1 to 15, with 1 being the highest priority. Unused network clocks are given a priority value of 0.
BITS	Selects the Building Integrated Timing Supply (BITS) clock input.
SYNCE *port-number*	Selects the clock input uplink port. For *port number:* • Enter 0 for input from TenGigabitEthernet 0/1. • Enter 1 for input from TenGigabitEthernet 0/2.

Defaults

The SyncE network clock is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

During normal operation, the reference clock is selected based on an algorithm that uses the priority rankings that you assign to the input clocks by using the **network-clock-select priority** *priority* global configuration command.

The reference clock source can be the BITS input or a PHY-recovered clock from one of the uplink ports. The ME 3800X and ME 3600X switch supports a BITS port through an RJ45 connector.

Examples

This example shows how to set the priority of a device to 2 and configure BITS as the clock input source.:

```
Switch(config)# network-clock-select 2 BITS
Switch(config)# exit
```

Related Commands

Command	Description
show network-clocks	Displays network clock configuration.
controller BITS commands	Configures the BITS clock controller characteristics.

network-clock-select hold-off timeout

To configure the time that the switch should wait if a Synchronous Ethernet (SyncE) reference clock goes down before removing it as the reference clock, use the **network-clock-select hold-off timeout** command in global configuration mode. To return to the default value, use the **no** form of this command.

network-clock-select hold-off timeout *value*

no network-clock-select hold-off timeout

Syntax Description

value	Sets the time in milliseconds. The accepted values are 0 or 50 to 10000 milliseconds (ms). The default is 300 ms.

Defaults

The default hold-off time is 300 ms.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

This command is supported only if you enter the **ql-enabled rep-segment** command in global configuration mode to configure the Resilient Ethernet Protocol (REP) workaround for resiliency and to avoid timing loops.

Setting a hold-off timeout ensures that the short activation of a signal failure is not passed to the clock selection process.

Examples

This example shows how to set the hold-off timeout to 5000 milliseconds:

```
Switch(config)# network-clock-select hold-off timeout 5000
Switch(config)# exit
```

Related Commands

Command	Description
show network-clocks	Displays network clock configuration.

network-clock-select hold-timeout

To configure the time after which the switch moves from the holdover state to the free-run state for system timing, use the **network-clock-select hold-timeout** command in global configuration mode. To return to the default value, use the **no** form of this command.

network-clock-select hold-timeout {*value* | **infinite**}

no network-clock-select hold-timeout

Syntax Description

value	Sets the time in seconds before the switch changes to a different clock input. The range is 0 to 86,400 seconds. This can be selected only when Resilient Ethernet Protocol (REP) quality level is enabled.
infinite	Sets the time to infinite. The switch continues to use the existing clock input information forever. This is the default.

Defaults

The default holdout time is infinite.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If there is no reliable clock source available, the switch goes into holdover mode and *replays* the saved clock from the last source.

You can configure a holdout time only if you enter the **ql-enabled rep-segment** command in global configuration mode to configure the Resilient Ethernet Protocol (REP) workaround for resiliency and to avoid timing loops.

When the configured holdout time expires, the switch goes into free-run state, where the timing clock is internal to the switch.

If you do not configure the REP workaround, the holdout time in a priority-based configuration is infinite.

Examples

This example shows how to set the switch to wait for 10,000 seconds after no reliable clock source is available and use the saved clock information:

```
Switch(config)# network-clock-select hold-timeout 10000
Switch(config)# exit
```

Related Commands

Command	Description
show network-clocks	Displays network clock configuration.

network-clock-select mode

To configure the Synchronous Ethernet (SyncE) input clock to determine the action to take if clock reference with higher priority than the selected reference clock becomes available, use the **network-clock-select mode** command in global configuration mode. To return to the default value, use the **no** form of this command.

network-clock-select mode {**nonrevert | revert**}

no network-clock-select mode {**nonrevert | revert**}

Syntax Description

nonrevert	Specifies that a new clock with higher priority does not immediately become the reference clock. In this mode, the new clock becomes the reference clock only if the current reference clock becomes invalid.
revert	Specifies that a new clock with higher priority is immediately selected as the new reference clock. This is the default.

Defaults

The default clock-select mode is revert.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

An input reference clock can be either forced or selected by an automatic selection algorithm based on the highest priority valid input clock. In revert mode, the forces clock automatically becomes the selected reference. In non-revertive mode, the forced clock becomes the selected reference only if the existing reference is invalidated or made unavailable for selection.

You can use the **set network-clocks** privileged EXEC command for more configuration of not-revertive mode.

Examples

This example shows how to specify that if an input with higher priority becomes valid, it immediately becomes the reference clock:

```
Switch(config)# network-clock-select mode revert
Switch(config)# exit
```

Related Commands

Command	Description
show network-clocks	Displays network clock configuration.

network-clock-select option

To configure the Synchronous Ethernet (SyncE) Ethernet Equipment Clock (EEC) option, use the **network-clock-select option** command in global configuration mode. To select the other (nonconfigured) option (E1 or T1), use the **no** form of this command.

network-clock-select option {**option1 | option2**}

no network-clock-select option {**option1 | option2**}

Syntax Description

option1	Selects 20.48 MHz (E1) as the input clock rate.
option2	Selects 1.544 MHz (T1) as the input clock rate.

Defaults

The default option is E1.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You should base the selected option on the timing format of the area of deployment.

After selecting the clock option, you can use the **controller BITS** global configuration commands to specify the line characteristics. Before using the controller BITS command to change the E1/T1 settings, you should ensure that the selection matches the option in this command.

Examples

This example shows how to select the E1 (2.048 MHz) clock option:

```
Switch(config)# network-clock-select option option1
Switch(config)# exit
```

Related Commands

Command	Description
show network-clocks	Displays network clock configuration.
controller BITS commands	Configures the BITS clock controller characteristics.

network-clock-select output

To set the priority and select the line interfaces to drive the output clock, use the **network-clock-select output** command in global configuration mode. To remove the configuration, use the **no** form of this command.

network-clock-select output *priority* **SYNCE** *port*

no network-clock-select output *priority*

Syntax Description

priority	Sets the priority of the device as a network clock. The range is from 1 to 15, with 1 being the highest priority. Unused network clocks are given a priority value of 0.
SYNCE *port*	Selects the clock output uplink port. For *port number:* • Enter 0 for input from TenGigabitEthernet 0/1. • Enter 1 for input from TenGigabitEthernet 0/2.

Defaults

Output clock priority is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The output clock (T4 or BITS OUT) is driven only on uplink ports.

The clock is not driven by the Building Integrated Timing Supply (BITS) or the system clock (T0).

Examples

This example shows how to set the BITS output priority to 2 on TenGigabitEthernet port 0/1.

```
Switch(config)# network-clock-select output 2 SYNCE 0.
Switch(config)# exit
```

Related Commands

Command	Description
show network-clocks	Displays network clock configuration.

network-clock-select wait-to-restore-timeout

To configure the time that the switch waits before a previously failed Synchronous Ethernet (SyncE) input clock must be fault-free before it is considered available as a synchronization source, use the **network-clock-select wait-to-restore timeout** command in global configuration mode. To return to the default value, use the **no** form of this command.

network-clock-select wait-to-restore timeout *value*

no network-clock-select wait-to-restore timeout

Syntax Description

value	Sets the wait time in seconds. The range is 0 to 720 seconds. The default is 300 seconds.

Defaults

SyncE wait to restore time is 300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can configure a holdout time only if you configure the REP quality level by entering the **ql-enabled rep-segment** command.

Examples

This example shows how to set the wait to restore time to 500 seconds:

```
Switch(config)# network-clock-select wait-to-restore timeout 500
Switch(config)# exit
```

Related Commands

Command	Description
ql-enabled rep-segment *segment-id*	Enable the Resilient Ethernet Protocol quality level workaround.
show network-clocks	Displays network clock configuration.

oam protocol cfm svlan

To configure the Ethernet virtual connection (EVC) operation, administration, and maintenance (OAM) protocol as IEEE 801.2ag Connectivity Fault Management (CFM) and to identify the service provider VLAN-ID for a CFM domain level, use the **oam protocol cfm svlan** command in EVC configuration mode. To remove the OAM protocol configuration for the EVC, use the **no** form of this command.

oam protocol cfm svlan *vlan-id* **domain** *domain-name*

no oam protocol

Syntax Description

vlan-id	Service provider VLAN ID for CFM. The range is 1 to 4094.
domain *domain-name*	Identifies the CFM domain for the service provider VLAN ID. If the CFM domain does not exist, the command is rejected, and an error message appears.

Defaults

There are no service provider VLANs identified for an EVC.

Command Modes

EVC configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When you enter **domain** *domain-name*, the CFM domain must have already been created by entering the **ethernet cfm domain** *domain-name* **level** *level-id* global configuration command. If the CFM domain does not exist, the command is rejected, and an error message appears.

Examples

This example shows how to enter EVC configuration mode and to configure the OAM protocol as CFM:

```
Switch(config)# ethernet evc test1
Switch(config-evc)# oam protocol cfm svlan 22 domain Operator
```

Related Commands

Command	Description
ethernet evc *evc-id*	Defines an EVC and enters EVC configuration mode.
ethernet cfm domain	Defines a CFM domain and sets the domain level.

pagp learn-method

To learn the source address of incoming packets received from an EtherChannel port, use the **pagp learn-method** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

pagp learn-method {**aggregation-port** | **physical-port**}

no pagp learn-method

Syntax Description

aggregation-port	Specifies address learning on the logical port-channel. The switch sends packets to the source using any of the ports in the EtherChannel. This setting is the default. With aggregate-port learning, it is not important on which physical port the packet arrives.
physical-port	Specifies address learning on the physical port within the EtherChannel. The switch sends packets to the source using the same port in the EtherChannel from which it learned the source address. The other end of the channel uses the same port in the channel for a particular destination MAC or IP address.

Defaults

The default is aggregation-port (logical port channel).

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When configuring **pagp learn-method**, learn must be configured to the same method at both ends of the link.

- The switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports.
- When the link partner to the switch is a physical learner, we recommend that you configure the switch as a physical-port learner. Use the **pagp learn-method physical-port** interface configuration command, and set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Only use the **pagp learn-method** interface configuration command in this situation.

You can verify the configuration by entering the **show running-config** privileged EXEC command or the **show pagp** *channel-group-number* **internal** privileged EXEC command.

Examples

This example shows how to set the learning method to learn the address on the physical port within the EtherChannel:

```
Switch(config-if)# pagp learn-method physical-port
```

This example shows how to set the learning method to learn the address on the port-channel within the EtherChannel:

```
Switch(config-if)# pagp learn-method aggregation-port
```

Related Commands

Command	Description
pagp port-priority	Selects a port over which all traffic through the EtherChannel is sent.
show pagp	Displays PAgP channel-group information.
show running-config	Displays the operating configuration.

pagp port-priority

To select a port over which all Port Aggregation Protocol (PAgP) traffic through the EtherChannel is sent, use the **pagp port-priority** command in interface configuration mode. If all unused ports in the EtherChannel are in hot-standby mode, they can be placed into operation if the currently selected port and link fails. To return to the default setting, use the **no** form of this command.

pagp port-priority *priority*

no pagp port-priority

Syntax Description

priority	A priority number ranging from 0 to 255.

Defaults

The default is 128.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The physical port with the highest operational priority and that has membership in the same EtherChannel is the one selected for PAgP transmission.

- The switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports.
- When the link partner to the switch is a physical learner, we recommend that you configure the switch as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command and to set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Use the **pagp learn-method** interface configuration command only in this situation.

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show pagp** *channel-group-number* **internal** privileged EXEC command.

Examples

This example shows how to set the port priority to 200:

```
Switch(config-if)# pagp port-priority 200
```

Related Commands

Command	Description
pagp learn-method	Provides the ability to learn the source address of incoming packets.
show pagp	Displays PAgP channel-group information.
show running-config	Displays the operating configuration.

permit (MAC access-list configuration)

To allow non-IP traffic to be forwarded if the conditions are matched, use the **permit** command in MAC access-list configuration mode. To remove a permit condition from the extended MAC access list, use the **no** form of this command.

{**permit** | **deny**} {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **cos** *cos* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**]

no {**permit** | **deny**} {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **cos** *cos* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** |**vines-ip** | **xns-idp**]

Note Though visible in the command-line help strings, **appletalk** is not supported as a matching condition.

Syntax Description

any	Keyword to specify to deny any source or destination MAC address.
host *src-MAC-addr* | *src-MAC-addr mask*	Defines a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied.
host *dst-MAC-addr* | *dst-MAC-addr mask*	Defines a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied.
type mask	(Optional) Uses the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. • *type* is 0 to 65535, specified in hexadecimal. • *mask* is a mask of *don't care* bits applied to the Ethertype before testing for a match.
aarp	(Optional) Selects Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber	(Optional) Selects EtherType DEC-Amber.
cos *cos*	(Optional) Selects an arbitrary class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message appears if the **cos** option is configured.
dec-spanning	(Optional) Selects EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv	(Optional) Selects EtherType DECnet Phase IV protocol.
diagnostic	(Optional) Selects EtherType DEC-Diagnostic.
dsm	(Optional) Selects EtherType DEC-DSM.
etype-6000	(Optional) Selects EtherType 0x6000.
etype-8042	(Optional) Selects EtherType 0x8042.
lat	(Optional) Selects EtherType DEC-LAT.
lavc-sca	(Optional) Selects EtherType DEC-LAVC-SCA.

lsap *lsap-number mask*	(Optional) Uses the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet. The *mask* is a mask of *don't care* bits applied to the LSAP number before testing for a match.
mop-console	(Optional) Selects EtherType DEC-MOP Remote Console.
mop-dump	(Optional) Selects EtherType DEC-MOP Dump.
msdos	(Optional) Selects EtherType DEC-MSDOS.
mumps	(Optional) Selects EtherType DEC-MUMPS.
netbios	(Optional) Selects EtherType DEC- Network Basic Input/Output System (NETBIOS).
vines-echo	(Optional) Selects EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	(Optional) Selects EtherType VINES IP.
xns-idp	(Optional) Selects EtherType Xerox Network Systems (XNS) protocol suite.

To filter IPX traffic, you use the *type mask* or **lsap** *lsap mask* keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in Table 2-3.

Table 2-3 IPX Filtering Criteria

IPX Encapsulation Type		
Cisco IOS Name	**Novell Name**	**Filter Criterion**
arpa	Ethernet II	Ethertype 0x8137
snap	Ethernet-snap	Ethertype 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

Defaults

This command has no defaults. However, the default action for a MAC-named ACL is to deny.

Command Modes

MAC access-list configuration

Command History

Release	**Modification**
12.2(52)EY	This command was introduced.

Usage Guidelines

You enter MAC access-list configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **any** or **host** keywords, you must enter an address mask.

After an access control entry (ACE) is added to an access control list, an implied **deny**-**any**-**any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

You can verify the configuration by entering the **show access-lists** privileged EXEC command.

Note For more information about MAC-named extended access lists, see the software configuration guide for this release.

Examples

This example shows how to define the MAC-named extended access list to allow NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is allowed.

```
Switch(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

This example shows how to remove the permit condition from the MAC-named extended access list:

```
Switch(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

This example permits all packets with Ethertype 0x4321:

```
Switch(config-ext-macl)# permit any any 0x4321 0
```

Related Commands

Command	Description
deny (MAC access-list configuration)	Denies non-IP traffic to be forwarded if conditions are matched.
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.
show access-lists	Displays access control lists configured on a switch.

police

To define a policer for classified traffic and to enter policy-map class police configuration mode, use the **police** command in policy-map class configuration mode. A policer defines an average traffic rate, a committed information rate (CIR), a peak information rate (PIR), and an action to take if a maximum is exceeded. In policy-map class police configuration mode, you can specify multiple actions for a packet. To remove a policer, use the **no** form of this command.

police {*rate-bps* | **cir** {*cir-bps* [*burst-bytes*] [**bc** *burst-bytes*] | **percent** *percent* [*burst-ms*] [**bc** *burst-ms*]} [**pir** {*pir-bps* [**be** *peak-burst*] | **percent** *percent* [**be** *peak-ms*]}] [*action*] [**conform-action** {**drop** | **set-cos-transmit** *new cos-value* | **set-discard-class-transmit** *new discard-value* | **set-dscp-transmit** *new dscp-value* | **set-mpls-exp-imposition-transmit** *new-imposition-exp-value* | **set-mpls-exp-topmost transmit** *new-topmost-exp-value* | **set-prec-transmit value** *new prec-value* | **set-qos-transmit value** *new qos-value*| **transmit**}] [**exceed-action** {**drop** | **set-cos-transmit** *new cos-value* | **set-discard-class-transmit** *new discard-value* | **set-dscp-transmit** *new dscp-value* | **set-mpls-exp-imposition-transmit** *new-imposition-exp-value* | **set-mpls-exp-topmost transmit** *new-topmost-exp-value* | **set-prec-transmit value** *new prec-value* | **set-qos-transmit value** *new qos-value*| **transmit**}] [**violate-action** {**drop** | **set-cos-transmit** *new cos-value* | **set-discard-class-transmit** *new discard-value* | **set-dscp-transmit** *new dscp-value* | **set-mpls-exp-imposition-transmit** *new-imposition-exp-value* | **set-mpls-exp-topmost transmit** *new-topmost-exp-value* | **set-prec-transmit value** *new prec-value* | **set-qos-transmit value** *new qos-value*| **transmit**}]

no police {*rate-bps* | **cir** {*cir-bps* [*burst-bytes*] [**bc** *burst-bytes*] | **percent** *percent* [*burst-ms*] [**bc** *burst-ms*]} [**pir** {*pir-bps* [**be** *peak-burst*] | **percent** *percent* [**be** *peak-ms*]}] [*action*] [**conform-action** {**drop** | **set-cos-transmit** *new cos-value* | **set-discard-class-transmit** *new discard-value* | **set-dscp-transmit** *new dscp-value* | **set-mpls-exp-imposition-transmit** *new-imposition-exp-value* | **set-mpls-exp-topmost transmit** *new-topmost-exp-value* | **set-prec-transmit value** *new prec-value* | **set-qos-transmit value** *new qos-value*| **transmit**}] [**exceed-action** {**drop** | **set-cos-transmit** *new cos-value* | **set-discard-class-transmit** *new discard-value* | **set-dscp-transmit** *new dscp-value* | **set-mpls-exp-imposition-transmit** *new-imposition-exp-value* | **set-mpls-exp-topmost transmit** *new-topmost-exp-value* | **set-prec-transmit value** *new prec-value* | **set-qos-transmit value** *new qos-value*| **transmit**}] [**violate-action** {**drop** | **set-cos-transmit** *new cos-value* | **set-discard-class-transmit** *new discard-value* | **set-dscp-transmit** *new dscp-value* | **set-mpls-exp-imposition-transmit** *new-imposition-exp-value* | **set-mpls-exp-topmost transmit** *new-topmost-exp-value* | **set-prec-transmit value** *new prec-value* | **set-qos-transmit value** *new qos-value*| **transmit**}]

Syntax Description

rate-bps	Specifies the average traffic rate in bits per second (b/s). The range is 64000 to 10000000000.
cir	Committed information rate (CIR) used for policing traffic.
cir-bps	CIR rate in b/s. The range is 64000 to 10000000000 b/s.
burst-bytes	(Optional) Specifies the normal burst size in bytes. The range is from 8000 to 16000000.
bc *burst- bytes*	(Optional) Conform burst. The number of acceptable burst bytes. The range is 8000 to 1000000 bytes.
cir percent *percent*	Specifies the CIR as a percentage of the bandwidth assigned to the class. The range is from 1 to 100 percent.

burst-ms	(Optional) Specifies the normal burst size in milliseconds. The range is 1 to 2000.
bc *burst-ms*	(Optional) Specifies the conformed burst (bc) in milliseconds. The range is 1 to 2000.
pir *pir-bps*	(Optional) Specifies the peak information rate (PIR) for the policy. The range is 64000 to 10000000000. This parameter is used for configuring a 2-rate, 3-color policer. If you do not enter a **pir** *pir-bps*, the policer is configured as a 1-rate, 2-color policer.
be *burst-bytes*	(Optional) Specifies the peak burst size in bytes. The range is 8000 to 16000000 bytes. The default is internally calculated based on the user configuration. You cannot configure this option unless you have entered the **pir** keyword.
pir percent *percent*	Specifies the PIR as a percentage of the bandwidth assigned to the class. The range is from 1 to 100 percent. if you enter **cir percent**, you must enter **pir** in **percent.**
be *burst-ms*	(Optional) Specifies the peak burst in milliseconds. The range is 1 to 2000.
conform-action	(Optional) Specifies the action to perform on packets that conform to the CIR and PIR. The default is **transmit**.
drop	(Optional) Drops the packet.
set-cos-transmit *new-cos-value*	Set a new class of service (CoS) value for the packet and send the packet. The range for the new CoS value is 0 to 7.
set-discard-class-transmit *new discard-value*	Sets a new discard-class value for the packet and send the packet. The range for the value is 0 to 7.
set-dscp-transmit *new-dscp-value*	Sets a new Differentiated Services Code Point (DSCP) value for the packet and send the packet. The range for the new DCSP value is 0 to 63.
set-mpls-exp-topmost transmit *new-topmost-exp-value*	Sets an MPLS label using the new MPLS EXP value at tag imposition, and send the packet. The range is 0 to 7.
set-mpls-exp-topmost transmit *new-topmost-exp-value*	Sets an MPLS label using the new MPLS EXP value for the topmost (outer) MPLS label, and send the packet. The range is 0 to 7.
set-prec-transmit *new-precedence-value*	Sets a new IP precedence value for the packet and send the packet. The range for the new IP precedence value is 0 to 7.
set-qos-transmit *qos-group-value*	Sets a new quality of service (QoS) group value for the packet and send the packet. The range for the new QoS value is 0 to 99.
transmit	(Optional) Sends the packet unmodified.
exceed-action	(Optional) Action to be taken for packets that exceed the CIR but are less than or equal to the PIR.
violate-action	(Optional) Action to be taken for packets exceed the PIR.

Defaults

No policers are defined.

Conform burst (**bc**) is automatically configured to 250 ms at the configured CIR.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can enter a single conform-action, exceed-action, or violate-action as part of the command string following the police command. You can also press Enter after the **police** command to enter policy-map class police configuration mode, where you can enter multiple actions. In policy-map class police configuration mode, you must enter an action to take.

The switch also supports marking multiple QoS parameters for the same class and simultaneously configuring conform-action, exceed-action, and violate-action marking.

The switch supports single-rate policing with a 2-color marker, or a 2-rate policer with a 3-color marker. Mapped packets can be sent without modification, dropped, or marked to options specified by the set command. Note that traffic rates are configured in bits per second and burst size is entered in bytes.

You can configure policing for any number of classes on any one of the three levels of the policy-map hierarchy. If you configure marking on one level, you can configure policing without marking (transmit, drop) on another level.

The ME 3600X switch supports 2000 policers. The number of policers supported on the ME 3800X switch is either 8000 or 16000, depending on the switch license.

An output policy map should match only the modified values of the out-of-profile traffic and not the original values.

When you define the policer and press Enter, you enter policy-map class police configuration mode, in which you can configure multiple policing actions. These commands are available:

- **conform-action**
- **exceed-action**
- **violate-action**
- **exit**: exits from QoS policy-map class police configuration mode. If you do not want to set multiple actions, you can enter **exit** without entering any other policy-map class police commands.
- **no**: negates or sets the default values of a command.

You can verify the configuration by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how to create a traffic classification with a CoS value of 4, create a policy map, and attach it to an ingress port. The average traffic rate is limited to 10000000 b/s with a burst size of 10000 bytes:

```
Switch(config)# class-map video-class
Switch(config-cmap)# match cos 4
Switch(config-cmap)# exit
Switch(config)# policy-map video-policy
Switch(config-pmap)# class video-class
Switch(config-pmap-c)# police 10000000 10000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy input video-policy
Switch(config-if)# exit
```

This example shows how to create policy map with a conform action of **set dscp** and a default exceed action, and attach it to an EFP.

```
Switch(config)# class-map in-class-1
Switch(config-cmap)# match dscp 14
Switch(config-cmap)# exit
Switch(config)# policy-map in-policy
Switch(config-pmap)# class in-class-1
Switch(config-pmap-c)# police 230000 8000 conform-action set-dscp-transmit 33
exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# service-policy input in-policy
Switch (config-if-srv)# exit
```

This example shows how to use policy-map class police configuration mode to set multiple conform actions and an exceed action. The policy map sets a committed information rate of 23000 bits per second (b/sb/s) and a conform burst size of 10000 bytes. The policy map includes multiple conform actions (for DSCP and for Layer 2 CoS) and an exceed action.

```
Switch(config)# class-map cos-set-1
Switch(config-cmap)# match cos 3
Switch(config-cmap)# exit
Switch(config)# policy-map map1
Switch(config-pmap)# class cos-set-1
Switch(config-pmap-c)# police cir 23000 bc 10000
Switch(config-pmap-c-police)# conform-action set-dscp-transmit 48
Switch(config-pmap-c-police)# conform-action set-cos-transmit 5
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy input map1
Switch(config-if)# exit
```

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
conform-action	Defines multiple actions for a policy-map class for packets that meet the CIR and the PIR.
exceed-action	Defines multiple actions for a policy-map class for packets that exceed the CIR but are less than or equal to the PIR.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
violate-action	Defines multiple actions for a policy-map class for packets that exceed the PIR.
show policy-map	Displays QoS policy maps.

policy-map

To create or to modify a policy map that can be attached to multiple physical ports and to enter policy-map configuration mode, use the **policy-map** command in global configuration mode. To delete an existing policy map, use the **no** form of this command.

policy-map *policy-map-name*

no policy-map *policy-map-name*

Syntax Description

policy-map-name	Name of the policy map.

Defaults

No policy maps are defined. By default, packets are sent unmodified.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The switch supports a maximum of 1024 unique policy maps.

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created or modified. Entering the **policy-map** command also enables the policy-map configuration mode, in which you can configure or modify the class policies for that policy map.

After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**: the specified traffic classification for which the policy actions are applied. The classification is defined in the **class-map** global configuration command. For more information, see the **class-map** command.
- **description**: describes the policy map (up to 200 characters).
- **exit**: exits policy-map configuration mode and returns to global configuration mode.
- **no**: removes a previously defined policy map.

Note If you enter the **no** policy-map configuration command or the **no policy-map** *policy-map-name* global configuration command to delete a policy map that is attached to an interface, a warning message appears that lists any interfaces (physical interfaces or Ethernet flow points (EFPs) from which the policy map is being detached. The policy map is then detached and deleted. For example:

```
Warning: Detaching Policy test1 from Interface GigabitEthernet0/1
```

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. You define packet classification on a physical-port basis.

You can create input policy maps and output policy maps, and you can assign one input policy map and one output policy map to a target (port or EFP service instance). The input policy map acts on incoming traffic on the port; the output policy map acts on outgoing traffic.

You can apply the same policy map to multiple targets.

Follow these guidelines when configuring input policy maps:

- The total number of input policy maps that can be attached to interfaces on the switch is limited by the availability of hardware resources. If you attempt to attach an input policy map that would exceed any hardware resource limitation, the configuration fails.
- You cannot configure an IP (IP standard and extended ACL, DSCP or IP precedence) and a non-IP (MAC ACL or CoS) classification within the same policy map, either within a single class map or across class maps within the policy map.
- These commands are not supported on input policy maps: **match discard-class** command, **match qos-grou**p command, **bandwidth** command for Class-Based-Weighting-Queuing (CBWFQ), **priority** command for class-based priority queueing, **queue-limit** command for Weighted Tail Drop (WTD), **shape average** command for port shaping, or class-based traffic shaping.

Follow these guidelines when configuring output policy maps:

- Output policy maps can have a maximum of eight classes, one of which is **class-default**, when the classes in the policy map are of class-level classification, such as **cos**, **dscp**, and **mpls exp**. There are no restrictions for classes in a VLAN-level policy map as long as the number does not exceed that supported by the license installed on the switch.
- Each class of a policy map can have three unique queue-limit configurations, including an unqualified queue-limit (that is a queue-limit without any qualifier). The switch supports a maximum of eight queues per policy map, including the class-default. Queue-limit configurations are unique for a class of a policy map. There are a total of 256 queue-limit profiles in the switch, some of which are default profiles. Each profile can have three queue-limit configurations. When queue-limit configurations are the same across classes, the classes use the same queue-limit profile.
- All output policy maps must include the same number of class maps (one to three) and the same classification (that is, the same class maps).

You can verify your settings by entering the **show policy-map** privileged EXEC command.

For more information about policy maps, see the software configuration guide for this release.

Examples

This example shows how to create an input policy map for three classes:

```
Switch(config)# policy-map input-all
Switch(config-pmap)# class gold
Switch(config-pmap-c)# set dscp af43
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver
Switch(config-pmap-c)# police 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze
Switch(config-pmap-c)# police 20000000
Switch(config-pmap-c)# exit
```

This example shows how to delete the policy map *input-all*:

```
Switch(config)# no policy-map input-all
```

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
service-policy (interface and service-instance configuration modes)	Applies a policy map to a port.
show policy-map	Displays quality of service (QoS) policy maps.

port-channel load-balance

To set the load-distribution method among the ports in the EtherChannel, use the **port-channel load-balance** command in global configuration mode. To return to the default setting, use the **no** form of this command.

port-channel load-balance {**dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac**}

no port-channel load-balance

Syntax Description

dst-ip	Load distribution is based on the destination host IP address.
dst-mac	Load distribution is based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.
src-dst-ip	Load distribution is based on the source and destination host IP address.
src-dst-mac	Load distribution is based on the source and destination host MAC address.
src-ip	Load distribution is based on the source host IP address.
src-mac	Load distribution is based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.

Defaults

The default is **src-mac**.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52EY	This command was introduced.

Usage Guidelines

For information about when to use these forwarding methods, see the "Configuring EtherChannels" chapter in the software configuration guide for this release.

You can verify the configuration by entering the **show running-config** privileged EXEC command or the **show etherchannel load-balance** privileged EXEC command.

Examples

This example shows how to set the load-distribution method to **dst-mac**:

```
Switch(config)# port-channel load-balance dst-mac
```

Related Commands

Command	Description
interface port-channel	Accesses or creates the port channel.
show etherchannel	Displays EtherChannel information for a channel.
show running-config	Displays the operating configuration.

port-type

To configure the port type on a Cisco ME switch, use the **port-type** command in interface configuration mode. Since all ports are network node interfaces (NNIs), this command has no effect.

port-type {**eni** | **nni** | **uni**}

no port-type

Syntax Description

eni	Enhanced network interface.
nni	Network node interface.
uni	User network interface.

Defaults

All ports are NNIs

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

All ports on the switch are NNIs. This command has no effect.

Related Commands

Command	Description
show port-type	Displays the port type of an interface.

priority

To configure class-based priority queuing for a class of traffic belonging to an output policy map, use the **priority** command in policy-map class configuration mode. To remove a priority specified for a class, use the **no** form of this command.

priority

no priority

Syntax Description

This command has no arguments or keywords.

Defaults

No policers are defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **priority** command assigns traffic to a low-latency path and ensures that packets belonging to the class have the lowest possible latency. Packets in the priority queue are scheduled and sent until the queue is empty.

Note Only one unique class map in an attached policy map can be associated with a **priority** command. You cannot configure priority along with any other queuing action (**bandwidth** or **shape average**).

Note You should exercise care when using the **priority** command. Excessive use of strict priority queuing might cause congestion in other queues.

You can associate the **priority** command only with a single unique class for all attached output policies on the switch.

You cannot associate the **priority** command with the **class-default** of the output policy map.

You cannot configure priority and any other scheduling action (**shape average** or **bandwidth**) in the same class.

All output classes and queues use a default queue-limit (see the queue-limit command). However, you can override the default value by explicitly configuring an unqualified queue-limit on the class of an output policy map. You can change the queue limit by using the **queue-limit** policy-map class command, overriding the default set by the **priority** command.

You can verify the configuration by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how to configure the class *out-class1* as a strict priority queue so that all packets in that class are sent before any other class of traffic. Other traffic queues are configured so that *out-class-2* gets 50 percent of the remaining bandwidth and *out-class3* gets 20 percent of the remaining bandwidth. The class **class-default** receives the remaining 30 percent with no guarantees.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
police	Defines a policer for classified traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays quality of service (QoS) policy maps.

ql-enabled rep-segment

To configure a Synchronous Ethernet (SyncE) Resilient Ethernet Protocol (REP) workaround for network resiliency and to avoid timing loops when there are any network failures within the REP segment, use the **ql-enabled rep-segment** command in global configuration mode. To disable the workaround, use the **no** form of this command.

ql-enabled rep-segment *segment-id*

no ql-enabled rep-segment

Syntax Description

segment-id	Specifies the SyncE REP segment to be used for the ESMC SSM workaround. The segment ID range is 1 to 1024.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Some SyncE networks use Ethernet Synchronous Messaging Channel (ESMC) with source-specific multicast (SSM) to ensure that the highest quality level clock available is selected and to prevent timing loops in the network. Because ESMC SSM is not supported on the switch, we recommend configuring the SyncE network as a REP segment to provide a REP workaround.

If you do not configure a REP workaround, an intermittent failure or change in network topology can cause timing loops in the SyncE network. Configuring REP allows the segment to automatically respond to a failure in the ring and avoid timing loops by changing the direction of the reference clock path.

SyncE uses REP only for failure detection, and not for timing topology discovery or timing loop prevention. Timing loops can still occur if port priority is not correctly configured.

You can see if a REP segment is enabled by entering the **show network-clocks** privileged EXEC command.

See the software configuration guide for more information about configuring REP segments and configuring the REP workaround.

Examples

This example shows how to configure the REP segment 3 as the quality-level workrooms.

```
Switch(config)# dl-enabled segment 3
```

Related Commands

Command	Description
network-clock-select	Configures the network clock for the switch.
show network-clocks	Displays SyncE configuration on the switch.

queue-limit

To set the queue maximum threshold for Weighted Tail Drop (WTD) in an output policy map, use the **queue-limit** command in policy-map class configuration mode. To return to the default, use the **no** form of this command.

queue-limit {*limit* [**bytes** *bytes* | **us** *microseconds*] | **cos** *value* | **discard-class** *value* | **dscp** *value* | **exp** *value* | **precedence** *value* | **qos-group** *value*}

no queue-limit {*limit* [**bytes** | **us**] | **cos** *value* | **discard-class** *value* | **dscp** *value* | **exp** *value* | **precedence** *value* | **qos-group** *value*}

Syntax Description

limit [**bytes** | **us**]	The threshold limit: • For **bytes** *bytes,* enter the maximum threshold in bytes. The range is from 200 to 491520. The default depends on the interface speed. On 10/100/1000 Mb/s interfaces, the default is approximately 12000 bytes. On 10 Gb/s interfaces, the default is approximately 120000 bytes. • For **us** *microseconds*, enter the maximum threshold in microseconds. This is the default for specifying threshold. The range is from 1 to 3932. The default depends on the interface: 10 Mb/s interfaces: 10000 us, 100 Mb/s interfaces: 1000 us, 1000 Mb/s and 10 Gb/s interfaces: 100 us. If you do not enter **bytes** *bytes or* **us** *microseconds*, the default is **us**.
cos *value*	Specifies a cost of service (CoS) value. The range is from 0 to 7.
discard-class *value*	Specifies a drop precedence for a packet during congestion management. The range is 0 to 7. This is the preferred way to specify a subclass within a queue to establish drop preference based on a queue buffer thresholds.
dscp *value*	Specifies a Differentiated Services Code Point (DSCP) value. The range is from 0 to 63.
exp *value*	Specifies an MPLS exponential value. The range is from 0 to 7.
precedence *value*	Specifies an IP precedence value. The range is from 0 to 7.
qos-group *value*	Specifies a quality-of-service (QoS) group value. The range is from 0 to 99.

Defaults

Default queue limits depend on the interface:

- 10 Mb/s interfaces: 10000 us or 12 KB
- 100 Mb/s interfaces: 1000 us or 12KB
- 1000 Mb/s interfaces: 100 us or 12 KB
- 10 Gb/s interfaces: 100 us or 120 KB

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You use the **queue-limit** policy-map class command to control output traffic. Queue-limit settings are not supported in input policy maps.

Use the other classification values to specify the subtype of traffic that needs to be mapped to the unique threshold on the queue.

The switch supports one output policy map for each interface. Each class of a policy map can have three unique queue-limit configurations, including an unqualified queue-limit (that is a queue-limit without any qualifier).

The switch supports a maximum of eight queues per policy map, including the class-default. Queue-limit configurations are unique for a class of a policy map. There are a total of 256 queue-limit profiles in the switch, some of which are default profiles. Each profile can have three queue-limit configurations. When queue-limit configurations are the same across classes, the classes use the same queue-limit profile.

If you try to attach an output policy map that contains a fourth queue-limit configuration to an interface, you see an error message and the attachment is not allowed.

The **queue-limit** command is supported only after you first configure a scheduling action, such as **bandwidth**, **shape-average**, or **priority**, except when you configure **queue-limit** in the **class-default** of an output policy map.

You cannot configure more than two unique threshold values for WTD qualifiers (**cos**, **dscp**, **precedence**, **exp**, **discard-class**, or **qos-group**) in the **queue-limit** command. However, you can map any number of qualifiers to those thresholds. You can configure a third unique threshold value to set the threshold for the queue, using the **queue-limit** command with no qualifiers.

You can use these same queue-limit values in multiple output policy maps on the switch. However, changing one of the queue-limit values in a class would create a new, unique queue-limit configuration. You can attach only three unique queue-limit configurations in output policy maps to interfaces at any one time. If you try to attach an output policy map with a fourth unique queue-limit configuration, you see this error message:

```
QoS: Configuration failed. Maximum number of allowable unique queue-limit
configurations exceeded.
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Examples

This example shows a policy map with a specified bandwidth and queue size. Traffic that is not DSCP 30 or 10 is assigned a queue-limit of 2000 bytes. Traffic with a DSCP value of 30 is assigned a queue-limit of 1000 bytes, and traffic with a DSCP value of 10 is assigned a queue limit of 1500 bytes. All traffic not belonging to the class traffic is classified into **class-default**, which is configured with 10 percent of the total available bandwidth and a large queue size of 3000 bytes.

```
Switch(config)# policy-map gold-policy
Switch(config-pmap)# class traffic
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# queue-limit bytes 2000
Switch(config-pmap-c)# queue-limit dscp 30 bytes 1000
Switch(config-pmap-c)# queue-limit dscp 10 bytes 1500
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 10
```

```
Switch(config-pmap-c)# queue-limit bytes 3000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output gold-policy
Switch(config-if)# exit
```

There can be only three unique qualified queue-limit thresholds. In this example, there are four unique thresholds, so the configuration is rejected:

```
Switch(config-pmap-c)# queue-limit 100 us
Switch(config-pmap-c)# queue-limit cos 2 200 us
Switch(config-pmap-c)# queue-limit cos 3 300 us
Switch(config-pmap-c)# queue-limit cos 4 400 us
```

In the next example, although there appear to be only three unique thresholds, in reality there are four threshold configurations, including an implied default threshold. The configuration is rejected.

```
Switch(config-pmap-c)# queue-limit cos 2 200 us
Switch(config-pmap-c)# queue-limit cos 3 300 us
Switch(config-pmap-c)# queue-limit cos 4 400 us
```

In this example, only three unique thresholds are configured and the configuration is allowed.

```
Switch(config-pmap-c)# queue-limit 100 us
Switch(config-pmap-c)# queue-limit cos 2 100 us
Switch(config-pmap-c)# queue-limit cos 3 300 us
Switch(config-pmap-c)# queue-limit cos 4 400 us
```

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays QoS policy maps.

random-detect

To configure WRED for a class in a policy map, use the **random-detect** command in policy-map class configuration mode. To disable WRED, use the **no** form of this command.

random-detect [**dscp-based** | **prec-based**|**cos-based**]

no random-detect

Syntax Description

dscp-based	(Optional) Specifies that WRED is to use the differentiated services code point (DSCP) value when it calculates the drop probability for a packet.
prec-based	(Optional) Specifies that WRED is to use the IP Precedence value when it calculates the drop probability for a packet.
cos-based	(Optional)Specifies that WRED is to use the Specific IEEE 802.1Q CoS values from 0 to 7

Command Default

WRED is disabled by default.

Command Modes

Policy-map class configuration when used in a policy map (config-pmap-c)

Command History

Release	Modification
15.1(2)EY	This command was introduced.

Usage Guidelines

Keywords

If you choose not to use either the **dscp-based** or the **prec-based** keywords, WRED uses the IP Precedence value (the default method) to calculate the drop probability for the packet.

WRED Functionality

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. WRED is most useful with protocols like Transport Control Protocol (TCP) that respond to dropped packets by decreasing the transmission rate.

The router automatically determines parameters to use in the WRED calculations. To change these parameters, use the **random-detect precedence** command.

WRED in a Policy Map

You can configure WRED as part of the policy map for a standard class or the default class. If you configure WRED, its packet drop capability is used to manage the queue when packets exceeding the configured maximum count are enqueued. If you configure the **queue-limit** command, tail drop is used.

To configure a policy map and create class policies, use the **policy-map** and **class** (policy-map) commands.

Two Methods for Calculating the Drop Probability of a Packet

This command includes two optional keywords, **dscp-based** and **prec-based**, that determine the method WRED uses to calculate the drop probability of a packet.

Note the following points when deciding which method to instruct WRED to use:

- With the **dscp-based** keyword, WRED uses the DSCP value (that is, the first six bits of the IP type of service (ToS) byte) to calculate the drop probability.
- With the **prec-based** keyword, WRED will use the IP Precedence value to calculate the drop probability.
- The **dscp-based** and **prec-based** keywords are mutually exclusive.
- If neither argument is specified, WRED uses the IP Precedence value to calculate the drop probability (the default method).

Examples

The following example configures the policy map called policy1 to contain policy specification for the class called class1. During times of congestion, WRED packet drop is used instead of tail drop.

```
! The following commands create the class map called class1:
class-map class1
 match input-interface fastethernet0/1

! The following commands define policy1 to contain policy specification for class1:
policy-map policy1
 class class1
  bandwidth 1000
  random-detect
```

The following example enables WRED to use the DSCP value 8. The minimum threshold for the DSCP value 8 is 24 and the maximum threshold is 40. This configuration was performed at the interface level.

```
Router(config)# interface serial0/0
Router(config-if)# random-detect dscp-based
Router(config-if)# random-detect dscp 8 24 40
```

The following example enables WRED to use the DSCP value 8 for class c1. The minimum threshold for DSCP value 8 is 24 and the maximum threshold is 40. The last line attaches the service policy to the output interface or virtual circuit (VC) p1.

```
Router(config-if)# class-map c1
Router(config-cmap)# match access-group 101
Router(config-if)# policy-map p1
Router(config-pmap)# class c1
Router(config-pmap-c)# bandwidth 48
Router(config-pmap-c)# random-detect dscp-based
Router(config-pmap-c)# random-detect dscp 8 24 40
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial0/0
Router(config-if)# service-policy output p1
```

Related Commands

Command	Description
random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.

Command	Description
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.

random-detect cos

To specify the outer class of service (CoS) value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling weighted random early detection (WRED), use the **random-detect cos** command in policy-map class configuration mode. To reset the thresholds and maximum probability denominator to the default values for the specified CoS, use the **no** form of this command.

random-detect cos *cos-value min-threshold max-threshold mark-probability-denominator*

no random-detect cos *cos-value min-threshold max-threshold mark-probability-denominator*

Syntax Description

cos-value	Specifies the CoS value. The CoS value ranges from 0 to 7.
min-threshold	Minimum threshold in number of packets. Valid values are 1 to 4096.
max-threshold	Maximum threshold in number of packets. Valid values are 1 to 4096.
mark-probabilit y-denominator	Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. Valid values are 1 to 65535.

Defaults

The default values for the *min-threshold* and *max-threshold* arguments are based on the output buffering capacity and the transmission speed for the interface.

The default value for the *mark-probability-denominator* argument is 10; 1 out of every 10 packets is dropped at the maximum threshold.

Command Modes

Policy-map class configuration

Command History

Release	Modification
15.1(2)EY	This command was introduced.

Usage Guidelines

Note the following points when using the **random-detect cos** command:

- When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified IP precedence.
- When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified IP precedence.
- The *mark-probability-denominator* argument is the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold.

Examples

In the following example, WRED has been enabled using the **random-detect cos** command. With the **random-detect cos** command, the CoS value has been specified, along with the minimum and maximum thresholds, and the maximum probability denominator.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policymap1
Router(config-pmap)# class class1
Router(config-pmap-c)# random-detect cos 1 12 25 1/10
Router(config-pmap-c)# end
```

Related Commands

Command	Description
random-detect cos-based	Enables WRED on the basis of the CoS value of a packet.

random-detect cos-based

To enable weighted random early detection (WRED) on the basis of the class of service (CoS) value of a packet, use the **random-detect cos-based** command in policy-map class configuration mode. To disable WRED, use the **no** form of this command.

random-detect cos-based *cos-value*

no random-detect cos-based

Syntax Description

cos-value	Specific IEEE 802.1Q CoS values from 0 to 7.

Command Default

When WRED is configured, the default minimum and maximum thresholds are determined on the basis of output buffering capacity and the transmission speed for the interface.

The default mark probability denominator is 10.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
15.1(2)EY	This command was introduced.

Examples

In the following example, WRED is configured on the basis of the CoS value. In this configuration, the **random-detect cos-based** command has been configured and a CoS value of 2 has been specified.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policymap1
Router(config-pmap)# class class1
Router(config-pmap-c)# random-detect cos-based 2
Router(config-pmap-c)# end
```

Related Commands

Command	Description
random-detect cos	Specifies the CoS value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling WRED.

random-detect dscp

To change the minimum and maximum packet thresholds for the differentiated services code point (DSCP) value, use the **random-detect dscp** command in QoS policy-map class configuration mode. To return the minimum and maximum packet thresholds to the default for the DSCP value, use the **no** form of this command.

random-detect dscp *dscp-value min-threshold max-threshold* [*mark-probability-denominator*]

no random-detect dscp *dscp-value min-threshold max-threshold* [*mark-probability-denominator*]

Syntax Description

dscp-value	The DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs7, ef**, or **rsvp**.
min-threshold	Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. When the average queue length reaches the minimum threshold, Weighted Random Early Detection (WRED) randomly drops some packets with the specified DSCP value.
max-threshold	Maximum threshold in number of packets. The value range of this argument is from the value of the *min-threshold* argument to 4096. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified DSCP value.
mark-probability-denominator	(Optional) Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. The value range is from 1 to 65536. The default is 10; 1 out of every 10 packets is dropped at the maximum threshold.

Command Default

If WRED is using the DSCP value to calculate the drop probability of a packet, all entries of the DSCP table are initialized with the default settings shown in Table 4 in the "Usage Guidelines" section of this command.

Command Modes

Policy-map class configuration

Command History

Release	Modification
15.1(2)EY	This command was introduced.

Usage Guidelines

The **random-detect dscp** command allows you to specify the DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, or **cs7**.

This command must be used in conjunction with the random-detect (interface) command.

Additionally, the random-detect dscp command is available only if you specified the dscp-based argument when using the random-detect (interface) command.

Default Values

Table 4 lists the default settings used by the random-detect dscp command for the DSCP value specified. Table 4 lists the DSCP value, and its corresponding minimum threshold, maximum threshold, and mark probability. The last row of the table (the row labeled "default") shows the default settings used for any DSCP value not specifically shown in the table.

Table 4 random-detect dscp Default Settings

DSCP (Precedence)	Minimum Threshold	Maximum Threshold	Mark Probability
af11	32	40	1/10
af12	28	40	1/10
af13	24	40	1/10
af21	32	40	1/10
af22	20	40	1/10
af23	24	40	1/10
af31	32	40	1/10
af32	28	40	1/10
af33	24	40	1/10
af41	32	40	1/10
af42	28	40	1/10
af43	24	40	1/10
cs1	22	40	1/10
cs2	24	40	1/10
cs3	26	40	1/10
cs4	28	40	1/10
cs5	30	40	1/10
cs6	32	40	1/10
cs7	34	40	1/10
ef	36	40	1/10
rsvp	36	40	1/10
default	20	40	1/10

Examples

The following example enables WRED to use the DSCP value of af22. The minimum threshold for the DSCP value af22 is 20, the maximum threshold is 40, and the mark probability is 10.

```
random-detect dscp af22 20 40 10
```

Related Commands

Command	Description
random-detect	Enables WRED

random-detect exponential-weighting-constant

To configure the exponential weight factor for the average queue size calculation for the queue reserved for a class, use the **random-detect exponential-weighting-constant** command in policy-map class configuration mode. To return the value to the default, use the **no** form of this command.

random-detect exponential-weighting-constant *exponent*

no random-detect exponential-weighting-constant

Syntax Description

exponent	Exponent from 1 to 16 used in the average queue size calculation.

Command Default

The default exponential weight factor is 9.

Command Modes

Policy-map class configuration

Command History

Release	Modification
15.1(2)EY	This command was introduced.

Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. WRED is most useful with protocols like TCP that respond to dropped packets by decreasing the transmission rate.

Use this command to configure the exponential weight factor for the average queue size calculation for the queue reserved for a class.

Examples

The following example configures the policy map called policy1 to contain policy specification for the class called class1. During times of congestion, WRED packet drop is used instead of tail drop. The weight factor used for the average queue size calculation for the queue for class1 is 12.

```
! The following commands create the class map called class1:
class-map class1
 match input-interface FE0/1

! The following commands define policy1 to contain policy specification for class1:
policy-map policy1
 class class1
 bandwidth 1000
 random-detect
 random-detect exponential-weighting-constant 12
```

The following example configures policy for a traffic class named int10 to configure the exponential weight factor as 12. This is the weight factor used for the average queue size calculation for the queue for traffic class int10. WRED packet drop is used for congestion avoidance for traffic class int10, not tail drop.

```
policy-map policy12
 class int10
 bandwidth 2000
 random-detect exponential-weighting-constant 12
```

Related Commands

Command	Description
random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
random-detect precedence	Configures WRED and DWRED parameters for a particular IP Precedence.

random-detect precedence

To configure WRED parameters for a particular IP Precedence for a class policy in a policy map, use the **random-detect precedence** command in policy-map class configuration mode. To return the values to the default for the precedence, use the **no** form of this command.

random-detect precedence *precedence_value min-threshold max-threshold mark-probability-denominator*

no random-detect precedence

Syntax Description

precedence	IP Precedence number. The value range is from 0 to 7.
min-threshold	Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified IP Precedence.
max-threshold	Maximum threshold in number of packets. The value range of this argument is from the value of the *min-threshold* argument to 4096. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified IP Precedence.
mark-probability-denominator	Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. The value range is from 1 to 65536. The default is 10; 1 out of every 10 packets is dropped at the maximum threshold.

Command Default

For all precedences, the *mark-probability-denominator* default is 10, and the *max-threshold* is based on the output buffering capacity and the transmission speed for the interface.

The default *min-threshold* depends on the precedence. The *min-threshold* for IP Precedence 0 corresponds to half of the *max-threshold*. The values for the remaining precedences fall between half the *max-threshold* and the *max-threshold* at evenly spaced intervals. See Table 5 in the "Usage Guidelines" section of this command for a list of the default minimum threshold values for each IP Precedence.

Command Modes

Policy-map class configuration (config-pmap-c)

Command History

Release	Modification
15.1(2) EY	This command was introduced.

Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists.

When you configure the **random-detect** command on a policy class, packets are given preferential treatment based on the IP Precedence of the packet. Use the **random-detect precedence** command to adjust the treatment for different precedences.

If you want WRED to ignore the precedence when determining which packets to drop, enter this command with the same parameters for each precedence. Remember to use reasonable values for the minimum and maximum thresholds.

Table 5 lists the default minimum threshold value for each IP Precedence.

Table 5 Default WRED and DWRED Minimum Threshold Values

	Minimum Threshold Value (Fraction of Maximum Threshold Value)	
IP Precedence	**WRED**	**DWRED**
0	9/18	8/16
1	10/18	9/16
2	11/18	10/16
3	12/18	11/16
4	13/18	12/16
5	14/18	13/16
6	15/18	14/16
7	16/18	15/16

Examples

The following example configures policy for a class called acl10 included in a policy map called policy10. Class acl101 has these characteristics: a minimum of 2000 kbps of bandwidth are expected to be delivered to this class in the event of congestion and a weight factor of 10 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop. IP Precedence is reset for levels 0 through 4.

```
policy-map policy10
class acl10
 bandwidth 2000
 random-detect
 random-detect exponential-weighting-constant 10
 random-detect precedence 0 32 256 100
 random-detect precedence 1 64 256 100
 random-detect precedence 2 96 256 100
 random-detect precedence 3 120 256 100
 random-detect precedence 4 140 256 100
```

Related Commands

Command	Description
bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
random-detect dscp	Changes the minimum and maximum packet thresholds for the DSCP value.
random-detect exponential-weighting-constant	Configures the WRED and DWRED exponential weight factor for the average queue size calculation.

rep admin vlan

To configure a Resilient Ethernet Protocol (REP) administrative VLAN for REP to transmit hardware flood layer (HFL) messages, use the **rep admin vlan** command in global configuration mode. To return to the default configuration with VLAN 1 as the administrative VLAN, use the **no** form of this command.

rep admin vlan *vlan-id*

no rep admin vlan

Syntax Description

vlan-id	The VLAN ID range is from 1 to 4094. The default is VLAN 1; the range to configure is 2 to 4094.

Defaults

The administrative VLAN is VLAN 1.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If the VLAN does not already exist, this command does not create the VLAN.

To avoid the delay introduced by relaying messages in software for link-failure or VLAN-blocking notification during load balancing, REP floods packets at the hardware flood layer (HFL) to a regular multicast address. These messages are flooded to the whole network, not just the REP segment. Switches that do not belong to the segment treat them as data traffic. Configuring an administrative VLAN for the whole domain can control flooding of these messages.

If no REP administrative VLAN is configured, the default is VLAN 1.

There can be only one administrative VLAN on a switch and on a segment.

You can verify the configuration by entering the **show interface rep detail** privileged EXEC command.

Examples

This example shows how to configure VLAN 100 as the REP administrative VLAN:

```
Switch (config)# rep admin vlan 100
```

Related Commands

Command	Description
show interfaces rep detail	Displays detailed REP configuration and status for all interfaces or the specified interface, including the administrative VLAN.

rep block port

To configure Resilient Ethernet Protocol (REP) VLAN load balancing, use the **rep block port** command in interface configuration mode on the REP primary edge port. To return to the default configuration, use the **no** form of this command.

rep block port {id *port-id* **|** *neighbor_offset* **| preferred} vlan {*vlan-list* | all}**

no rep block port {**id** *port-id* **|** *neighbor_offset* **| preferred**}

Syntax Description

id *port-id*	Identifies the VLAN blocking alternate port by entering the unique port ID that is automatically generated when REP is enabled. The REP port ID is a 16-character hexadecimal value. You can view the port ID for an interface by entering the **show interface** *interface-id* **rep detail** command.
neighbor_offset	Identifies the VLAN blocking alternate port by entering the offset number of a neighbor. The range is –256 to +256; a value of 0 is invalid. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors.
preferred	Identify the VLAN blocking alternate port as the segment port on which you entered the **rep segment** *segment-id* **preferred** interface configuration command. **Note** Entering the **preferred** keyword does not ensure that the preferred port is the alternate port; it gives it preference over other similar ports.
vlan	Identifies the VLANs to be blocked.
vlan-list	Specifies a VLAN ID from 1 to 4094 or a range or sequence of VLANs (such as 1-3, 22, 41-44) of VLANs to be blocked.
all	Specifies to block all VLANs.

Defaults

The default behavior after you enter the **rep preempt segment** privileged EXEC command (for manual preemption) is to block all VLANs at the primary edge port. This behavior remains until you configure the **rep block port** command.

If the primary edge port cannot determine which port is to be the alternate port, the default action is no preemption and no VLAN load balancing.

Command Modes

Interface configuration

Command History

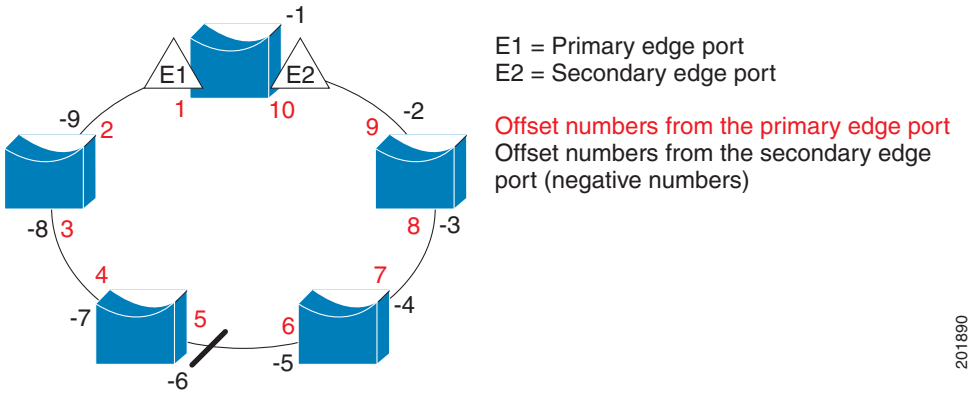
Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You must enter this command on the REP primary edge port.

When you select an alternate port by entering an offset number, this number identifies the downstream neighbor port of an edge port. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors. See Figure 2-1.

Figure 2-1 Neighbor Offset Numbers in a REP Segment



Note You would never enter an offset value of 1 because that is the offset number of the primary edge port itself.

If you have configured a preempt delay time by entering the **rep preempt delay** *seconds* interface configuration command and a link failure and recovery occurs, VLAN load balancing begins after the configured preemption time period elapses without another link failure. The alternate port specified in the load-balancing configuration blocks the configured VLANs and unblocks all other segment ports. If the primary edge port cannot determine the alternate port for VLAN balancing, the default action is no preemption.

Each port in a segment has a unique port ID. The port ID format is similar to the one used by the spanning tree algorithm: a port number (unique on the bridge) associated to a MAC address (unique in the network). To determine the port ID of a port, enter the **show interface** *interface-id* **rep detail** privileged EXEC command.

Examples

This example shows how to configure REP VLAN load balancing on the Switch B primary edge port (Gigabit Ethernet port 0/1) and to configure Gigabit Ethernet port 0/2 of Switch A as the alternate port to block VLANs 1 to 100. The alternate port is identified by its port ID, shown in bold in the output of the **show interface rep detail** command for the Switch A port.

```
Switch A# show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB17800EEE
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 1
Preempt Delay Timer: 35 sec
Load-balancing block port: none
Load-balancing block vlan: none
```

```
STCN Propagate to:
PDU/TLV statistics:
LSL PDU rx: 107122, tx: 192493

Switch B# config t
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# rep block port id 0080001647FB1780 vlan 1-100
Switch (config-if)# exit
```

This example shows how to configure VLAN load balancing by using a neighbor offset number and how to verify the configuration by entering the **show interfaces rep detail** privileged EXEC command:

```
Switch# config t
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep block port 6 vlan 1-110
Switch (config-if)# end

Switch# show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB178009C3
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 3
Preempt Delay Timer: 35 sec
Load-balancing block port: 6
Load-balancing block vlan: 1-110
STCN Propagate to: none
LSL PDU rx: 1466780, tx: 3056637
HFL PDU rx: 2, tx: 0
BPA TLV rx: 1, tx: 2119695
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 757406, tx: 757400
EPA-COMMAND TLV rx: 1, tx: 1
EPA-INFO TLV rx: 178326, tx: 178323
```

Related Commands

Command	Description
rep preempt delay	Configures a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.
rep preempt segment	Manually starts REP VLAN load balancing on a segment.
show interfaces rep detail	Displays REP detailed configuration and status for all interfaces or the specified interface, including the administrative VLAN.

rep lsl-age-timer

To configure the Link Status Layer (LSL) age timer for the time period that the Resilient Ethernet Protocol (REP) interface remains up without receiving a hello from the REP neighbor, use the **rep lsl-age-timer** command in interface configuration mode on a REP port. To return to the default time, use the **no** form of this command.

rep lsl-age timer *value*

no rep lsl-age timer

Syntax Description

value	The age-out time in milliseconds. The range is from 920 to 10000 ms in 40-ms increments. The default is 5000 ms (5 seconds).

Defaults

The REP link shuts down if it does not receive a hello message from a neighbor for 5000 ms.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The LSL hello timer is set to the age-timer value divided by 3 so that there should be at least two LSL hellos sent during the LSL age timer period. If no hellos are received within that time, the REP link shuts down.

In Cisco IOS Release 12.2(52)SE, the LSL age-timer range changed from 3000 to 10000 ms in 500-ms increments to 120 to 10000 ms in 40-ms increments. If the REP neighbor device is not running Cisco IOS Release 12.2(52)SE or later, you must use the shorter time range because the device does not accept values out of the earlier range.

EtherChannel port channel interfaces do not support LSL age-timer values less than 1000 ms. If you try to configure a value less than 1000 ms on a port channel, you receive an error message and the command is rejected.

You can verify the configured ageout time by entering the **show interfaces rep detail** privileged EXEC command.

Examples

This example shows how to configure the REP LSL age timer on a REP link to 7000 ms:

```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep lsl-age-timer 7000
Switch (config-if)# exit
```

Related Commands

Command	Description
show interfaces rep [**detail**]	Displays REP configuration and status for all interfaces or the specified interface, including the configured LSL age-out timer value.

rep preempt delay

To configure a waiting period after a segment port failure and recovery before Resilient Ethernet Protocol (REP) VLAN load balancing is triggered, use the **rep preempt delay** command in interface configuration mode on the REP primary edge port. To remove the configured delay, use the **no** form of this command.

rep preempt delay *seconds*

no rep preempt delay

Syntax Description

seconds	Sets the number of seconds to delay REP preemption. The range is 15 to 300.

Defaults

No preemption delay is set. If you do not enter the **rep preempt delay** command, the default is manual preemption with no delay.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You must enter this command on the REP primary edge port.

You must enter this command and configure a preempt time delay if you want VLAN load balancing to automatically trigger after a link failure and recovery.

If VLAN load balancing is configured, after a segment port failure and recovery, the REP primary edge port starts a delay timer before VLAN load balancing occurs. Note that the timer restarts after each link failure. When the timer expires, the REP primary edge alerts the alternate port to perform VLAN load balancing (configured by using the **rep block port** interface configuration command) and prepares the segment for the new topology. The configured VLAN list is blocked at the alternate port, and all other VLANs are blocked at the primary edge port.

You can verify the configuration by entering the **show interfaces rep** privileged EXEC command.

Examples

This example shows how to configure a REP preemption time delay of 100 seconds on the primary edge port:

```
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# rep preempt delay 100
Switch (config-if)# exit
```

Related Commands

Command	Description
rep block port	Configures VLAN load balancing.
show interfaces rep	Displays REP configuration and status for all interfaces or a specified interface.

rep preempt segment

To manually start Resilient Ethernet Protocol (REP) VLAN load balancing on a segment, use the **rep preempt segment** command in privileged EXEC mode.

rep preempt segment *segment_id*

Syntax Description

segment-id	ID of the REP segment. The range is from 1 to 1024.

Defaults

Manual preemption is the default behavior.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When you enter the **rep preempt segment** *segment-id* command, a confirmation message appears before the command is executed because preemption can cause network disruption.

Enter this command on the switch on the segment that has the primary edge port.

If you do not configure VLAN load balancing, entering this command results in the default behavior—the primary edge port blocks all VLANs.

You configure VLAN load balancing by entering the **rep block port** {**id** *port-id* | *neighbor_offset* | **preferred**} **vlan** {*vlan-list* | **all**} interface configuration command on the REP primary edge port before you manually start preemption.

There is not a **no** version of this command.

Examples

This example shows how to manually trigger REP preemption on segment 100 with the confirmation message:

```
Switch)# rep preempt segment 100
The command will cause a momentary traffic disruption.
Do you still want to continue? [confirm]
```

Related Commands

Command	Description
rep block port	Configures VLAN load balancing.
show interfaces rep [**detail**]	Displays REP configuration and status for all interfaces or the specified interface.

rep segment

To enable Resilient Ethernet Protocol (REP) on an interface and to assign a segment ID to it, use the **rep segment** command in interface configuration mode. To disable REP on the interface, use the **no** form of this command.

rep segment *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]

no rep segment

Syntax Description

segment-id	Assigns a segment ID to the interface. The range is from 1 to 1024.
edge	(Optional) Identifies the interface as one of the two REP edge ports. Entering the **edge** keyword without the **primary** keyword configures the port as the secondary edge port.
no-neighbor	(Optional) Configures a segment edge with no external REP neighbor.
primary	(Optional) On an edge port, specifies that the port is the primary edge port. A segment has only one primary edge port. If you configure two ports in a segment as the primary edge port, for example ports on different switches, the REP selects one of them to serve as the segment primary edge port.
preferred	(Optional) Specifies that the port is the preferred alternate port or the preferred port for VLAN load balancing. **Note** Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.

Defaults

REP is disabled on the interface.

When REP is enabled on an interface, the default is for the port to be a regular segment port.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

REP ports must be Layer 2 trunk ports.

REP ports should not be configured as access ports.

You must configure two edge ports on each REP segment, a primary edge port and a port to act as a secondary edge port. If you configure two ports in a segment as the primary edge port, for example ports on different switches, the configuration is allowed, but the REP selects one of them to serve as the segment primary edge port.

- REP ports follow these rules:
  - There is no limit to the number of REP ports on a switch; however, only two ports on a switch can belong to the same REP segment.
  - If only one port on a switch is configured in a segment, the port should be an edge port.
  - If two ports on a switch belong to the same segment, they must be both edge ports, both regular segment ports, or one regular port and one edge no-neighbor port. An edge port and regular segment port on a switch cannot belong to the same segment.
  - If two ports on a switch belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.

If you configure two ports in a segment as the primary edge port, for example ports on different switches, the REP selects one of them to serve as the segment primary edge port. Enter the **show rep topology** privileged EXEC command on a port in the segment to verify which port is the segment primary edge port.

REP interfaces come up in a blocked state and remain in a blocked state until notified that it is safe to unblock. You need to be aware of this to avoid sudden connection losses.

You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

In networks where ports on a neighboring switch do not support REP, you can configure the non-REP facing ports as edge no-neighbor ports. These ports inherit all properties of edge ports and you can configure them as any other edge port, including to send STP or REP topology change notices to the aggregation switch. In this case, the STP topology change notice (TCN) that is sent is a multiple spanning-tree (MST) STP message.

You can verify the configuration by entering the **show interfaces rep** privileged EXEC command. To verify which port in the segment is the primary edge port, enter the **show rep topology** privileged EXEC command.

When the **no-neighbor** keyword is specified the segment edge is configured with no external REP neighbor. However if **rep stcn stp** command is enabled MST will be enabled on the port.

Examples

This example shows how to enable REP on a regular (nonedge) segment port:

```
Switch (config)# interface gigabitethernet0/1
Switch (config-if)# rep segment 100
```

This example shows how to enable REP on a port and to identify the port as the REP primary edge port:

```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep segment 100 edge primary
```

This example shows how to configure the same configuration when the interface has no external REP neighbor:

```
Switch# configure terminal
Switch (conf)# interface gigabitethernet0/1
Switch (conf-if)# rep segment 100 edge no-neighbor primary
```

This example shows how to enable REP on a port and to identify the port as the REP secondary edge port:

```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep segment 100 edge
```

Related Commands

Command	Description
show interfaces rep [**detail**]	Displays REP configuration and status for all interfaces or the specified interface.
show rep topology [**detail**]	Displays information about all ports in the segment, including which one was configured and selected as the primary edge port.

rep stcn

To configure a port to send Resilient Ethernet Protocol (REP) segment topology change notifications (STCNs) to another interface, to other segments, or to Spanning Tree Protocol (STP) networks, use the **rep stcn** command in interface configuration mode on a REP edge port. To disable the sending of STCNs to the interface, segment, or STP network, use the **no** form of this command.

rep stcn {**interface** *interface-id* | **segment** *id-list* | **stp**}

no rep stcn {**interface** | **segment** | **stp**}

Syntax Description

interface *interface-id*	Identifies a physical interface or port channel to receive STCNs.
segment *id-list*	Identifies one REP segment or list of segments to receive STCNs. The range is 1 to 1024. You can also configure a sequence of segments (for example 3-5, 77, 100).
stp	Sends STCNs to an STP network.

Defaults

Transmission of STCNs to other interfaces, segments, or STP networks is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Enter this command on a segment edge port.

You use this command to notify other portions of the Layer 2 network of topology changes that occur in the local REP segment. This removes obsolete entries in the Layer 2 forwarding table in other parts of the network, which allows faster network convergence.

You can verify the configuration by entering the **show interfaces rep detail** privileged EXEC command.

When you configure **rep stcn stp** the STCNs are sent to an stp network. However where **no-neighbor** keyword is specified MST will be enabled on the port.

Examples

This example shows how to configure the REP primary edge port to send STCNs to segments 25 to 50:

```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# rep stcn segment 25-50
Switch (config-if)# exit
```

Related Commands

Command	Description
show interfaces rep [**detail**]	Displays REP configuration and status for all interfaces or the specified interface.

reserved-only

To allocate only reserved addresses in the Dynamic Host Configuration Protocol (DHCP) address pool, use the **reserved-only** command in DHCP pool configuration mode. to return to the default, use the **no** form of the command.

reserved-only

no reserved-only

Syntax Description

This command has no arguments or keywords.

Defaults

The default is to not restrict pool addresses

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Entering the **reserved-only** command restricts assignments from the DHCP pool to preconfigured reservations. Unreserved addresses that are part of the network or on pool ranges are not offered to the client, and other clients are not served by the pool.

By entering this command, users can configure a group of switches with DHCP pools that share a common IP subnet and that ignore requests from clients of other switches.

To access DHCP pool configuration mode, enter the **ip dhcp pool** *name* global configuration command.

Examples

This example shows how to configure the DHCP pool to allocate only reserved addresses:

```
Switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip dhcp pool test1
Switch(dhcp-config)# reserved-only
```

You can verify your settings by entering the **show ip dhcp pool** privileged EXEC command.

Related Commands

Command	Description
show ip dhcp pool	Displays the DHCP address pools.

reserved-only

rmon collection stats

To collect Ethernet group statistics, which include usage statistics about broadcast and multicast packets, and error statistics about cyclic redundancy check (CRC) alignment errors and collisions, use the **rmon collection stats** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

rmon collection stats *index* [**owner** *name*]

no rmon collection stats *index* [**owner** *name*]

Syntax Description

index	Remote Network Monitoring (RMON) collection control index. The range is 1 to 65535.
owner *name*	(Optional) Owner of the RMON collection.

Defaults

The RMON statistics collection is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The RMON statistics collection command is based on hardware counters.

Examples

This example shows how to collect RMON statistics for the owner *root*:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# rmon collection stats 2 owner root
```

Related Commands

Command	Description
show rmon statistics	Displays RMON statistics.

service instance

To configure an Ethernet service instance on the interface and to enter Ethernet service-instance configuration mode, use the **service instance** command in interface configuration mode. To delete the service instance, use the **no** form of this command.

service instance *id* **ethernet** [*evc-id*]

no service instance *id*

Syntax Description

id	Defines a service instance identifier, a per-interface service identifier that does not map to a VLAN. The range is 1 to 4000.
ethernet	Identifies the service instance as an Ethernet instance.
evc-id	(Optional) Attaches an Ethernet virtual connection (EVC) to the service instance.

Defaults

No Ethernet service instances are defined.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

After you enter the **service instance** *id* **ethernet** command, the switch enters Ethernet service configuration mode, and these configuration commands are available:

- **default**—sets the service instance to its default state.
- **description**—adds a specific description for the service instance.
- **encapsulation**—configures Ethernet frame match criteria.
- **errdisable recovery cause mac-security**—configure the error disable recovery timer interval from a MAC security violation.
- **ethernet lmi ce-vlan map**—configures Ethernet Local Management Interface (LMI) parameters. See the **ethernet lmi ce-vlan map** command.
- **exit**: exits EVC configuration mode and returns to global configuration mode.
- **l2prototol** {**peer** | **tunnel**}—configures Layer 2 control protocol processing.
- **mac security**—configures MAC address security.
- **no**— negates a command or returns a command to its default setting.
- **service-policy**—attach a policy map to the EFP.
- **shutdown**—shuts down the EFP (no shutdown brings up the EFP)

Examples

This example shows how to define an Ethernet service instance and to enter Ethernet service configuration mode for EVC *test*:

```
Switch(config-if)# service instance 333 ethernet test
Switch(config-if-srv)#
```

Related Commands

Command	Description
show ethernet service instance	Displays information about configured Ethernet service instances.

service password-recovery

To enable the password-recovery mechanism (the default), use the **service password-recovery** command in global configuration mode. This mechanism allows an end user with physical access to the switch to press the break key on the console terminal to interrupt the boot process while the switch is powering up and to assign a new password.

To disable part of the password-recovery functionality, use the **no** form of this command. When the password-recovery mechanism is disabled, interrupting the boot process is allowed only if the user agrees to set the system back to the default configuration.

service password-recovery

no service password-recovery

Syntax Description

This command has no arguments or keywords.

Defaults

The password-recovery mechanism is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

As a system administrator, you can use the **no service password-recovery** command to disable some of the functionality of the password recovery feature by allowing an end user to reset a password only by agreeing to return to the default configuration. This provides configuration file security by ensuring that only authenticated and authorized users have access to the configuration file and prevents users from accessing the configuration file by using the password recovery process.

The password recovery procedure requires using a break key. After the switch performs power-on self test (POST), the switch begins the autoboot process. The boot loader prompts the user for a break key character during the boot-up sequence, as shown in this example:

```
***** The system will autoboot in 5 seconds *****

Send a break key to prevent autobooting.
```

You must enter the break key on the console terminal within 5 seconds of receiving the message that the system will autoboot. A user with physical access to the switch presses the break key on the console terminal within 5 seconds of receiving the message that flash memory is initializing. The System LED flashes green until the **break key** is accepted. After the **break key** is accepted, the System LED turns off until after the switch boots.

If the password-recovery mechanism is disabled, this message appears:

```
The password-recovery mechanism has been triggered, but
is currently disabled. Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point. However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?
```

If the user chooses not to reset the system to the default configuration, the normal boot process continues as if the **break key** had not been pressed. If you choose to reset the system to the default configuration, the configuration file in flash memory is deleted, and the VLAN database file, *flash:vlan.dat* (if present), is deleted.

Note If you use the **no service password-recovery** command to control end user access to passwords, we recommend that you save a copy of the configuration file in a location away from the switch in case the end user uses the password recovery procedure and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch.

You can enter the **show version** privileged EXEC command to determine if password recovery is enabled or disabled.

Examples

This example shows how to disable password recovery on a switch so that a user can only reset a password by agreeing to return to the default configuration.

```
Switch(config)# no service-password recovery
Switch(config)# exit
```

Related Commands

Command	Description
show version	Displays version information for the hardware and firmware.

service-policy (interface and service-instance configuration modes)

To apply a policy map defined by the **policy-map** command to the incoming or outgoing traffic of a target, use the **service-policy** command in interface configuration mode or service-instance configuration mode. To remove the policy map and port association, use the **no** form of this command.

service-policy {**input** | **output**} *policy-map-name*

no service-policy {**input** | **output**} *policy-map-name*

Syntax Description

input	Applies the policy map to the input of a target (physical port or Ethernet flow point (EFP) service instance.
output	Applies the policy map to the output of a target.
policy-map-name	The specified policy map to be applied.

Defaults

No policy maps are attached to the port or service instance.

Command Modes

Interface configuration or service-instance configuration mode

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Only one input policy map and one output policy map can be attached to a target, which can be a physical interface or Ethernet flow point service instance.

The switch supports a limit of three unique queue-limit configurations across all output policy maps at any time. Multiple policy maps can share the same queue-limit configuration.If you try to attach an output policy map with a fourth unique queue-limit configuration, you see this error message:

```
QoS: Configuration failed. Maximum number of allowable unique queue-limit
configurations exceeded.
```

You can attach input or output policy maps to a Gigabit Ethernet port 10 Gigabit Ethernet port or to a service instance. You cannot attach policy maps to switch virtual interfaces (SVIs) and EtherChannel interfaces.

You can verify the configuration by entering the **show running-config** privileged EXEC command.

Examples

This example shows how to apply *plcmap1* as an output policy map to a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output plcmap1
```

This example shows how to remove *plcmap2* from a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no service-policy output plcmap2
```

This example shows how to apply *plcmap1* as an output policy map to a service instance:

```
Switch (config)# interface gigabitethernet0/2
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# service-policy output plcmap1
```

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays quality of service (QoS) policy maps.
show policy-map interface [*interface-id*]	Displays policy maps configured on the specified interface or on all interfaces.
show running-config	Displays the operating configuration.

set cos

To set a Layer 2 class of service (CoS) value in the packet, use the **set cos** command in policy-map class configuration mode. To remove traffic marking, use the **no** form of this command.

set cos *cos_value*

no set cos *cos_value*

Syntax Description

cos_value	Enters an IEEE 802.1Q class of service/user priority value with which to classify traffic. The range is from 0 to 7.

Defaults

No traffic marking is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can configure **set cos** with all other marking actions, specifically **set dscp**, **set discard-class**, **set mpls, set precedence**, and **set qos-group**, for the same class.

Use the **set cos** command if you want to mark a packet that is being sent to a switch. Switches can leverage Layer 2 header information including a CoS value marking.

You can use the **match cos** class-map configuration command and the **set cos** policy-map class configuration command together to allow switches to interoperate and provide quality of service (QoS) based on the CoS markings. You can also configure Layer 2 to Layer 3 mapping by matching on the CoS value because switches can already match and set CoS values.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how to set all FTP traffic to cos 3:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set cos 3
Switch(config-pmap-c)# exit
```

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays QoS policy maps.

set discard-class

To classify packets by entering the exact value to be marked for traffic to be discarded, use the **set discard-class** command in policy-map class configuration mode. To remove the discard-class value, use the **no** form of this command.

set discard-class *value*

no discard-class *value*

Syntax Description

value	Sets the value to be marked for discarding traffic. The range is from 0 to 7.

Defaults

No traffic marking is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can configure **set discard-class** with all other marking actions, specifically **set cos**, **set dscp**, **set mpls, set precedence**, and **set qos-group**, for the same class.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how to set all FTP traffic with a discard value of 5:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set discard-class 5
Switch(config-pmap-c)# exit
```

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays QoS policy maps.

set dscp

To mark IPv4 traffic by setting a Differentiated Services Code Point (DSCP) value in the type of service (ToS) byte of the packet, use the **set** [**ip**] **dscp** command in policy-map class configuration mode. To remove the traffic marking, use the **no** form of this command.

set [**ip**] **dscp** *dscp_value*

no set [**ip**] **dscp** *dscp_value*

Note Entering **ip dscp** is the same as entering **dscp**.

Syntax Description

dscp-value	Specifies a DSCP value with which to classify traffic. The range is from 0 to 63. You also can enter a mnemonic name for a commonly used value.

Defaults

No traffic marking is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can configure **set dscp** with other marking actions, specifically **set cos**, **set discard-class**, **set mpls,** and **set qos-group**, for the same class.

You cannot use the **set dscp** command with the **set precedence** command to mark the same packet. DSCP values and IP precedence values are mutually exclusive. A packet can have one value or the other, but not both.

After DSCP bits are set, other quality of service (QoS) features can then operate on the bit settings.

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the DSCP value at the edge of the network (or administrative domain) and data is then queued according to the precedence. Class-based weighted fair queuing (CBWFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Tail Drop (WTD) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Instead of using numeric values, you can also specify the *dscp-value* by using the reserved keywords **EF**, **AF11**, and **AF12**.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how to set all FTP traffic to DSCP 10:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
```

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays QoS policy maps.

set mpls

To set an multiprotocol label switching (MPLS) experimental (EXP) value in the inbound packet to classify packets, use the **set mpls** command in policy-map class configuration mode. To remove the group MPLS value, use the **no** form of this command.

set mpls experimental {**imposition | topmost**} *experimental _value*

no set mpls experimental {**imposition | topmost**} *experimental _value*

Syntax Description

imposition	Specifies that the MPLS experimental value is set at tag imposition. This means that the MPLS value in a packet header is set with the new value after the packet is switched. This applies only to MPLS packets that are MPLS routed, but to all MPLS tags that are imposed by the switch.
topmost	Specifies that the MPLS experimental value is set for the outermost or topmost label. This marks all valid MPLS packets.
experimental _value	Sets the MPLS value to use to classify traffic. The range is from 0 to 7.

Defaults

No traffic marking is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can configure **set mpls** with all other marking actions, specifically **set cos, set discard-class**, **set dscp**, **set qos-group**, and **set precedence**, for the same class.

In an MPLS network, packet IP precedence bits are copied into the MPLS EXP field at the edge of the network. If a service provider wants to set a QoS value for an MPLS packet to a different value, instead of overwriting the value in the IP precedence field that belongs to a customer, the service provider can set the MPLS experimental field. The IP header remains available for the customer's use, and the QoS of an IP packet is not changed as the packet travels through the MPLS network.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how to classify all MPLS packets with a value of 5:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class mpls_class
Switch(config-pmap-c)# set mpls topmost 5
Switch(config-pmap-c)# exit
```

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays QoS policy maps.

set network-clocks

To force selection of a particular Synchronous Ethernet (SyncE) network clock or to configure automatic clock selection, use the **set network-clocks** command in privileged EXEC mode.

set network-clocks {**automatic | force-select | next-select**}

Note There is not a **no** version of this command.

Syntax Description

automatic	Selects automatic clock selection. The clock with the highest priority is always automatically selected as the input clock.
force-select	Forces the system to reselect a valid network clock with the highest priority.
next-select	Forces the system to select the valid clock with the next highest priority.

Defaults

The default is automatic.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The input network clock reference selection can be forced or automatically selected using an algorithm based on the highest priority valid input clock.

- In revertive mode, the forced clock automatically becomes the selected reference.
- In non-revertive mode, the forced clock is selected only with the existing reference is invalidated or made unavailable.

You use the **network-clock-select mode** {**nonrevert | revert**} global configuration command to set the mode.

You can use **set network-clocks next-select** command to scroll through the set of available clocks.

After you force the network clock selection by entering the **set network-clocks force-select** or **set network-clocks next-select** command, the system remains locked to the selected clock even if it becomes invalid.

You can verify your settings by entering the **show network-clock** privileged EXEC command.

Examples

This example shows how to set clock selection to automatic:

```
Switch# set network-clocks automatic
```

Related Commands

Command	Description
network-clock-select	Configures the network clock for the switch.
show network-clocks	Displays SyncE configuration on the switch.

set precedence

To mark IPv4 traffic by setting an IP-precedence value in the packet, use the **set** [**ip**] **precedence** command in policy-map class configuration mode. To remove traffic marking, use the **no** form of this command.

set [**ip**] **precedence** *precedence_value-*

no set [**ip**] **precedence** *precedence_value*

Note Entering **ip precedence** is the same as entering **precedence**.

Syntax Description

precedence_value	Specifies an IPv4 precedence value with which to classify traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value. • **0** to **7**—Enter up to 4 precedence values separated by spaces. • **critical**—Match packets with critical precedence (5). • **flash**—Match packets with flash precedence (3). • **flash-override**—Match packets with flash override precedence (4). • **immediate**—Match packets with immediate precedence (2). • **internet**—Match packets with internetwork control precedence (6). • **network**—Match packets with network control precedence (7). • **priority**—Match packets with priority precedence (1). • **routine**—Match packets with routine precedence (0).

Defaults

No traffic marking is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can configure **set precedence** with other marking actions, specifically **set cos**, **set discard-class**, **set mpls, and set qos-group**, for the same class.

You cannot use the **set precedence** command with the **set dscp** command to mark the same packet. DSCP values and IP precedence values are mutually exclusive. A packet can have one value of the other, but not both.

After precedence bits are set, other quality of service (QoS) features can then operate on the bit settings.

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain) and data is then queued according to the precedence. Class-based weighted fair queuing (CBWFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Tail Drop (WTD) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how to give all FTP traffic an IP precedence value of 5:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set precedence 5
Switch(config-pmap-c)# exit
```

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays QoS policy maps.

set qos-group

To set a quality of service (QoS) group identifier that can be used later to classify packets, use the **set qos-group** command in policy-map class configuration mode. To remove the group identifier, use the **no** form of this command.

set qos-group *value*

no set qos-group *value*

Syntax Description

value	Sets the QoS group value to use to classify traffic. The range is from 0 to 99.

Defaults

No traffic marking is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can configure **set qos-group** with all other marking actions, specifically **set cos, set discard-class**, **set dscp**, **set mpls**, and **set precedence**, for the same class.

Use this command to associate a QoS group value with a traffic flow as it enters the switch, which can then be used in an output policy map to identify the flow.

A maximum of 100 QoS groups (0 through 99) is supported on the switch.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how to set all FTP traffic to QoS group 5:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set qos-group 5
Switch(config-pmap-c)# exit
```

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays QoS policy maps.

setup

To configure the switch with its initial configuration, use the **setup** command in privileged EXEC mode.

setup

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When you use the **setup** command, make sure that you have this information:

- IP address and network mask
- Password strategy for your environment

When you enter the **setup** command, an interactive dialog, called the System Configuration Dialog, appears. It guides you through the configuration process and prompts you for information. The values shown in brackets next to each prompt are the default values last set by using either the **setup** command facility or the **configure** privileged EXEC command.

Help text is provided for each prompt. To access help text, press the question mark (**?**) key at a prompt.

To return to the privileged EXEC prompt without making changes and without running through the entire System Configuration Dialog, press **Ctrl-C**.

When you complete your changes, the setup program shows you the configuration command script that was created during the setup session. You can save the configuration in NVRAM or return to the setup program or the command-line prompt without saving it.

Examples

This is an example of output from the **setup** command:

```
Switch# setup
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system.

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
```

```
Enter host name [Switch]:host-name

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: enable-secret-password

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: enable-password

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: terminal-password

  Configure SNMP Network Management? [no]: yes
  Community string [public]:

Current interface summary
Any interface listed with OK? value "NO" does not have a valid configuration

Interface                  IP-Address      OK? Method Status                Protocol
Vlan1                      172.20.135.202  YES NVRAM  up                    up

GigabitEthernet0/1         unassigned      YES unset  up                    up

GigabitEthernet0/2         unassigned      YES unset  up                    down

<output truncated>

Port-channel1              unassigned      YES unset  up                    down

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface vlan1:
Configure IP on this interface? [yes]: yes
IP address for this interface: ip_address
Subnet mask for this interface [255.0.0.0]: subnet_mask

The following configuration command script was created:

hostname host-name
enable secret 5 $1$LiBw$0Xc1wyT.PXPkuhFwqyhVi0
enable password enable-password
line vty 0 15
password terminal-password
snmp-server community public
!
no ip routing
!
interface GigabitEthernet0/1
no ip address
!
interface GigabitEthernet0/2
no ip address
!
end
```

```
Use this configuration? [yes/no]: yes
!
[0] Go to the IOS command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

Enter your selection [2]:
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
show version	Displays version information for the hardware and firmware.

shape average

To configure class-based or port shaping by specifying the average traffic shaping rate or percentage, use the **shape average** command in policy-map class configuration mode. To set port shaping, use the command with the class **class-default**. To remove traffic shaping, use the **no** form of this command.

shape average {*target bps* | **percent** *value*}

no shape average {*target bps* | **percent** *value*}

Syntax Description

target bps	Sets the target average rate in bits per second (bps). The range is from 1000 to 1000000000.
percent *value*	Sets the percentage of interface bandwidth. The range is 0 to 100 percent. The percentage is calculated based on the peak information rate (PIR) of the parent class. If there is no configured PIR at any level, this is the percentage of the interface speed. Setting the percent to 0 disables shaping.

Defaults

No traffic shaping is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You use the **shape average** policy-map class command to control output traffic. Shaping is not supported in input policy maps.

Traffic shaping limits the rate of transmission of data. Configuring traffic shaping for a user-defined class or **class-default** for class-based shaping sets the peak information rate (PIR) for that class. Configuring traffic shaping for the class **class-default** when it is the only class in the policy map that is attached to an interface sets the PIR for the interface (port shaping).

You cannot configure **shape average** in a class that includes priority queueing (configured with the **priority** policy-map class configuration command).

The **shape average** command uses a default queue limit for the class. You can change the queue limit by using the **queue-limit** policy-map class command, overriding the default that is set by the **shape average** command.

Port shaping is applied to all traffic leaving an interface. It uses a policy map with only class default when the maximum bandwidth for the port is specified by using the **shape average** command. A child policy can be attached to the class-default in a hierarchical policy map format to specify class-based and VLAN-based actions.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how to configure traffic shaping for outgoing traffic on a Gigabit Ethernet port so that *outclass1*, *outclass2*, and *outclass3* get a maximum of 50, 20, and 10 Mb/s of the available port bandwidth.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class classout1
Switch(config-pmap-c)# shape average 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout2
Switch(config-pmap-c)# shape average 20000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout3
Switch(config-pmap-c)# shape average 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

This example shows how to configure port shaping by configuring a hierarchical policy map that shapes a port to 90 Mb/s, allocated according to the *out-policy* policy map configured in the previous example.

```
Switch(config)# policy-map out-policy-parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# service-policy out-policy
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output out-policy-parent
Switch(config-if)# exit
```

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays QoS policy maps.
show policy-map interface [*interface-id*]	Displays policy maps configured on the specified interface or on all interfaces.

show access-lists

To display access control lists (ACLs) configured on the switch, use the **show access-lists** command in privileged EXEC mode.

show access-lists [*name* | *number* | **hardware counters** | **ipc**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

name	(Optional) Name of the ACL.
number	(Optional) ACL number. The range is 1 to 2699.
hardware counters	(Optional) Displays global hardware ACL statistics for switched and routed packets.
ipc	(Optional) Displays Interprocess Communication (IPC) protocol access-list configuration download information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help strings, the **rate-limit** keywords are not supported.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The switch supports only IP standard and extended access lists. Therefore, the allowed numbers are only 1 to 199 and 1300 to 2699.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show access-lists** command:

```
Switch# show access-lists
Standard IP access list 1
    10 permit 1.1.1.1
    20 permit 2.2.2.2
    30 permit any
    40 permit 0.255.255.255, wildcard bits 12.0.0.0
Standard IP access list videowizard_1-1-1-1
    10 permit 1.1.1.1
Standard IP access list videowizard_10-10-10-10
    10 permit 10.10.10.10
Extended IP access list 121
    10 permit ahp host 10.10.10.10 host 20.20.10.10 precedence routine
```

This is an example of output from the **show access-lists hardware counters** command:

```
Switch# show access-lists hardware counters
L2 ACL INPUT Statistics
     Drop:                All frame count: 855
     Drop:                All bytes count: 94143
     Drop And Log:        All frame count: 0
     Drop And Log:        All bytes count: 0
     Bridge Only:         All frame count: 0
     Bridge Only:         All bytes count: 0
     Bridge Only And Log: All frame count: 0
     Bridge Only And Log: All bytes count: 0
     Forwarding To CPU:   All frame count: 0
     Forwarding To CPU:   All bytes count: 0
     Forwarded:           All frame count: 2121
     Forwarded:           All bytes count: 180762
     Forwarded And Log:   All frame count: 0
     Forwarded And Log:   All bytes count: 0

 L3 ACL INPUT Statistics
     Drop:                All frame count: 0
     Drop:                All bytes count: 0
     Drop And Log:        All frame count: 0
     Drop And Log:        All bytes count: 0
     Bridge Only:         All frame count: 0
     Bridge Only:         All bytes count: 0
     Bridge Only And Log: All frame count: 0
     Bridge Only And Log: All bytes count: 0
     Forwarding To CPU:   All frame count: 0
     Forwarding To CPU:   All bytes count: 0
     Forwarded:           All frame count: 13586
     Forwarded:           All bytes count: 1236182
     Forwarded And Log:   All frame count: 0
     Forwarded And Log:   All bytes count: 0

 L2 ACL OUTPUT Statistics
     Drop:                All frame count: 0
     Drop:                All bytes count: 0
     Drop And Log:        All frame count: 0
     Drop And Log:        All bytes count: 0
     Bridge Only:         All frame count: 0
     Bridge Only:         All bytes count: 0
     Bridge Only And Log: All frame count: 0
     Bridge Only And Log: All bytes count: 0
     Forwarding To CPU:   All frame count: 0
     Forwarding To CPU:   All bytes count: 0
     Forwarded:           All frame count: 232983
     Forwarded:           All bytes count: 16825661
     Forwarded And Log:   All frame count: 0
     Forwarded And Log:   All bytes count: 0
```

```
L3 ACL OUTPUT Statistics
    Drop:                All frame count: 0
    Drop:                All bytes count: 0
    Drop And Log:        All frame count: 0
    Drop And Log:        All bytes count: 0
    Bridge Only:         All frame count: 0
    Bridge Only:         All bytes count: 0
    Bridge Only And Log: All frame count: 0
    Bridge Only And Log: All bytes count: 0
    Forwarding To CPU:   All frame count: 0
    Forwarding To CPU:   All bytes count: 0
    Forwarded:           All frame count: 514434
    Forwarded:           All bytes count: 39048748
    Forwarded And Log:   All frame count: 0
    Forwarded And Log:   All bytes count: 0
```

Related Commands

Command	Description
access-list	Configures a standard or extended numbered access list on the switch.
ip access list	Configures a named IP access list on the switch.
mac access-list extended	Configures a named or numbered MAC access list on the switch.

show archive status

To display the status of a new image being downloaded to a switch with the HTTP or the TFTP protocol, use the **show archive status** command in privileged EXEC mode.

show archive status [**|**{**begin | exclude | include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If you use the **archive download-sw** privileged EXEC command to download an image to a TFTP server, the output of the **show archive status** command shows the status of the download.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

These are examples of output from the **show archive status** command:

```
Switch# show archive status
IDLE: No upgrade in progress

Switch# show archive status
LOADING: Upgrade in progress

Switch# show archive status
EXTRACT: Extracting the image

Switch# show archive status
VERIFY: Verifying software

Switch# show archive status
RELOAD: Upgrade completed. Reload pending
```

Related Commands

Command	Description
archive download-sw	Downloads a new image from a TFTP server to the switch.

show boot

To display the settings of the boot environment variables, use the **show boot** command in privileged EXEC mode.

show boot [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show boot** command.

```
Switch# show boot
5d05h: %SYS-5-CONFIG_I: Configured from console by console
BOOT path-list      :
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break        : no
Manual Boot         : yes
HELPER path-list    :
Auto upgrade        : yes
```

Table 3-6 show boot Field Descriptions

Field	Description
BOOT path-list	Displays a semicolon-separated list of executable files to load and execute when automatically booting. • If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory. • If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system.
Config file	Displays the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
Private Config file	Displays the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
Enable Break	Displays whether a break during booting is enabled or disabled. If it is set to yes, on, or 1, you can interrupt the automatic boot process by pressing the Break key on the console after the flash file system is initialized.
Manual Boot	Displays whether the switch automatically or manually boots. If it is set to no or 0, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the switch from the boot loader mode.
Helper path-list	Displays a semicolon separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.

Related Commands

Command	Description
boot config-file	Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
boot enable-break	Enables interrupting the automatic boot process.
boot manual	Enables manually booting the switch during the next boot cycle.
boot private-config-file	Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the private configuration.
boot system	Specifies the Cisco IOS image to load during the next boot cycle.

show cable-diagnostics tdr

To display the Time Domain Reflector (TDR) results, use the **show cable-diagnostics tdr** command in privileged EXEC mode.

show cable-diagnostics tdr interface *interface-id* [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	Specifies the interface on which TDR was run.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

TDR is supported only on copper Ethernet 10/100 ports on the Cisco ME switch. It is not supported on small form-factor pluggable (SFP)-module ports. For more information about TDR, see the software configuration guide for this release.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show cable-diagnostics tdr interface** *interface-id* command on a Cisco ME switch:

```
Switch# show cable-diagnostics tdr interface gigabitethernet0/1

TDR test last run on: March 01 18:14:44

Interface Speed Local pair Pair length        Remote pair Pair status
--------- ----- ---------- ------------------ ----------- --------------------
Gi0/1     100M  Pair A     4    +/- 5  meters Pair A      Normal
                Pair B     4    +/- 5  meters Pair B      Normal
                Pair C     N/A                Pair C      N/A
                Pair D     N/A                Pair D      N/A
```

Table 2-7 lists the descriptions of the fields in the **show cable-diagnostics tdr** command output.

Table 3-7 Fields Descriptions for the show cable-diagnostics tdr Command Output

Field	Description
Interface	Interface on which TDR was run.
Speed	Speed of connection.
Local pair	Name of the pair of wires that TDR is testing on the local interface.
Pair length	Location on the cable where the problem is, with respect to your switch. TDR can only find the location in one of these cases: • The cable is properly connected, the link is up, and the interface speed is 100 Mbps. • The cable is open. • The cable has a short.
Remote pair	Name of the pair of wires to which the local pair is connected. TDR can learn about the remote pair only when the cable is properly connected and the link is up.
Pair status	The status of the pair of wires on which TDR is running: • Normal—The pair of wires is properly connected. • Not completed—The test is running and is not completed. • Not supported—The interface does not support TDR. • Open—The pair of wires is open. • Shorted—The pair of wires is shorted. • ImpedanceMis—The impedance is mismatched. • Short/Impedance Mismatched—The impedance mismatched or the cable is short. • InProgress—The diagnostic test is in progress

This is an example of output from the **show interface** *interface-id* command when TDR is running:

```
Switch# show interface gigabitethernet0/1
gigabitethernet0/1 is up, line protocol is up (connected: TDR in Progress)
```

This is an example of output from the **show cable-diagnostics tdr interface** *interface-id* command when TDR is not running:

```
Switch# show cable-diagnostics tdr interface gigabitethernet0/1
% TDR test was never issued on gi0/1
```

If an interface does not support TDR, this message appears:

```
% TDR test is not supported on switch 1
```

Related Commands

Command	Description
test cable-diagnostics tdr	Enables and runs TDR on an interface.

show class-map

To display quality of service (QoS) class maps, which define the match criteria to classify traffic, use the **show class-map** command in user EXEC mode.

show class-map [*class-map-name*] [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

class-map-name	(Optional) Displays the contents of the specified class map.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show class-map** command:

```
Switch> show class-map
Class Map match-all videowizard_10-10-10-10 (id 2)
   Match access-group name videowizard_10-10-10-10

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-all dscp5 (id 3)
   Match ip dscp 5
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to the class whose name you specify.
match access-group	Defines the match criteria to classify traffic.

show controllers bits

To display the state of the Building Integrated Timing Supply (BITS) clock controller, use the **show controllers bits** in privileged EXEC mode.

show controllers bits [**|** {**begin | exclude | include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is a partial output example from the **show controllers bits** command:

```
Switch# show controllers BITS

Applique type is T1
Line Coding is B8ZS(Rx), B8ZS(Tx)
Framing is ESF(Rx), ESF(Tx)
Line Build Out is 0-133ft
No alarms detected.
```

Related Commands

Command	Description
controllers bits input applique	Sets the BITS clock input link type and characteristics.
controllers bits output applique	Sets the BITS clock output link type and characteristics.

show controllers cpu-interface

To display the state of the CPU network interface ASIC and the send and receive statistics for packets reaching the CPU, use the **show controllers cpu-interface** command in privileged EXEC mode.

show controllers cpu-interface [**|** {**begin | exclude | include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is a partial output example from the **show controllers cpu-interface** command:

```
Switch# show controllers cpu-interface

Queue cnt           normal     jumbo      normal-err jumbo-err  dropped    unfill
------------------------------------------------------------------------------
sw forwarding       0          0          0          0          0          0
routing protocol    0          0          0          0          0          0
icmp                0          0          0          0          0          0
host                0          0          0          0          0          0
acl logging         0          0          0          0          0          0
stp                 36         0          0          0          0          0
l2 protocol         14357      0          0          0          0          0
mcast control       18862      0          0          0          0          0
broadcast           0          0          0          0          0          0
rep                 0          0          0          0          0          0
cfm                 0          0          0          0          0          0
control?            0          0          0          0          0          0
ip mpls ttl         0          0          0          0          0          0
ipmcast default     0          0          0          0          0          0
route data          0          0          0          0          0          0
ipmcast mismatch    0          0          0          0          0          0
ipmcast rpf-fail    0          0          0          0          0          0
routing throttle    0          0          0          0          0          0
ipmcast?            0          0          0          0          0          0
<output truncated>
```

Related Commands

Command	Description
show controllers ethernet-controller	Displays per-interface send and receive statistics read from the hardware or the interface internal registers.
show interfaces	Displays the administrative and operational status of all interfaces or a specified interface.

show controllers ethernet-controller

To display per-interface send and receive statistics read from the hardware, use the **show controllers ethernet-controller** command in privileged EXEC mode without keywords. To display the interface internal registers, use with the **phy** keyword or use the **port-asic** keyword to display information about the port ASIC.

show controllers ethernet-controller [*interface-id*] [**down-when-looped**] [**phy** [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	The physical interface (including type, module, and port number).
down-when-looped	Display the state related to the down-when-looped detection.
phy	(Optional) Displays the status of the internal registers on the switch physical layer device (PHY) for the device or the interface. This display includes the operational state of the automatic medium-dependent interface crossover (Auto-MDIX) feature on an interface.
detail	(Optional) Displays details about the PHY internal registers.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC (only supported with the *interface-id* keywords in user EXEC mode)

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

This display without keywords provides traffic statistics, basically the RMON statistics for all interfaces or for the specified interface.

When you enter the **phy** keywords, the displayed information is useful primarily for Cisco technical support representatives troubleshooting the switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show controllers ethernet-controller** command for an interface. Table 2-8 describes the *Transmit* fields, and Table 2-9 describes the *Receive* fields.

```
Switch# show controllers ethernet-controller gigabitethernet0/1
Transmit GigabitEthernet0/1              Receive
      1279800 Bytes                          2788787 Bytes
            0 Unicast frames                   12058 Unicast frames
         4050 Multicast frames                 14779 Multicast frames
            0 Broadcast frames                  1195 Broadcast frames
            0 Dot1Q frames                         0 Dot1Q frames
            0 Too old frames                  771712 Unicast bytes
            0 Deferred frames                1934854 Multicast bytes
            0 MTU exceeded frames              82221 Broadcast bytes
            0 FCS errors                           0 FCS errors
            0 1 collision frames                   0 Alignment errors
            0 2 collision frames
            0 3 collision frames                   0 Oversize frames
            0 4 collision frames                   0 Undersize frames
            0 5 collision frames                   0 Collision fragments
            0 6 collision frames
            0 7 collision frames               12071 Minimum size frames
            0 8 collision frames               13917 65 to 127 byte frames
            0 9 collision frames                   0 128 to 255 byte frames
            0 10 collision frames               2044 256 to 511 byte frames
            0 11 collision frames                  0 512 to 1023 byte frames
            0 12 collision frames                  0 1024 to 1518 byte frames
            0 13 collision frames                  0 Overrun frames
            0 14 collision frames
            0 15 collision frames
            0 Pause frames                         0 Pause frames
            0 Excessive collisions                 0 Symbol error frames
            0 Late collisions                      0 Invalid frames, too large
            0 VLAN discard frames                  0 Valid frames, too large
            0 Excess defer frames                  0 Invalid frames, too small
            0 64 byte frames                       0 Valid frames, too small
            0 127 byte frames
            0 255 byte frames                      0 Too old frames
         4050 511 byte frames                      0 Valid oversize frames
            0 1023 byte frames                     0 System FCS error frames
            0 1518 byte frames
            0 Too large frames
            0 Good (1 coll) frames
            0 Good (>1 coll) frames
```

Table 3-8 Transmit Field Descriptions

Field	Description
Bytes	The total number of bytes sent on an interface.
Unicast Frames	The total number of frames sent to unicast addresses.
Multicast frames	The total number of frames sent to multicast addresses.
Broadcast frames	The total number of frames sent to broadcast addresses.
Too old frames	The number of frames dropped on the egress port because the packet aged out.
Deferred frames	The number of frames that are not sent after the time exceeds 2*maximum-packet time.
MTU exceeded frames	The number of frames that are larger than the maximum allowed frame size.
1 collision frames	The number of frames that are successfully sent on an interface after one collision occurs.
2 collision frames	The number of frames that are successfully sent on an interface after two collisions occur.

Table 3-8 Transmit Field Descriptions (continued)

Field	Description
3 collision frames	The number of frames that are successfully sent on an interface after three collisions occur.
4 collision frames	The number of frames that are successfully sent on an interface after four collisions occur.
5 collision frames	The number of frames that are successfully sent on an interface after five collisions occur.
6 collision frames	The number of frames that are successfully sent on an interface after six collisions occur.
7 collision frames	The number of frames that are successfully sent on an interface after seven collisions occur.
8 collision frames	The number of frames that are successfully sent on an interface after eight collisions occur.
9 collision frames	The number of frames that are successfully sent on an interface after nine collisions occur.
10 collision frames	The number of frames that are successfully sent on an interface after ten collisions occur.
11 collision frames	The number of frames that are successfully sent on an interface after 11 collisions occur.
12 collision frames	The number of frames that are successfully sent on an interface after 12 collisions occur.
13 collision frames	The number of frames that are successfully sent on an interface after 13 collisions occur.
14 collision frames	The number of frames that are successfully sent on an interface after 14 collisions occur.
15 collision frames	The number of frames that are successfully sent on an interface after 15 collisions occur.
Excessive collisions	The number of frames that could not be sent on an interface after 16 collisions occur.
Late collisions	After a frame is sent, the number of frames dropped because late collisions were detected while the frame was sent.
VLAN discard frames	The number of frames dropped on an interface because the CFI[1] bit is set.
Excess defer frames	The number of frames that are not sent after the time exceeds the maximum-packet time.
64 byte frames	The total number of frames sent on an interface that are 64 bytes.
127 byte frames	The total number of frames sent on an interface that are from 65 to 127 bytes.
255 byte frames	The total number of frames sent on an interface that are from 128 to 255 bytes.
511 byte frames	The total number of frames sent on an interface that are from 256 to 511 bytes.
1023 byte frames	The total number of frames sent on an interface that are from 512 to 1023 bytes.
1518 byte frames	The total number of frames sent on an interface that are from 1024 to 1518 bytes.
Too large frames	The number of frames sent on an interface that are larger than the maximum allowed frame size.
Good (1 coll) frames	The number of frames that are successfully sent on an interface after one collision occurs. This value does not include the number of frames that are not successfully sent after one collision occurs.

1. CFI = Canonical Format Indicator

Table 3-9 Receive Field Descriptions

Field	Description
Bytes	The total amount of memory (in bytes) used by frames received on an interface, including the FCS[1] value and the incorrectly formed frames. This value excludes the frame header bits.
Unicast frames	The total number of frames successfully received on the interface that are directed to unicast addresses.
Multicast frames	The total number of frames successfully received on the interface that are directed to multicast addresses.

Table 3-9 Receive Field Descriptions (continued)

Field	Description
Broadcast frames	The total number of frames successfully received on an interface that are directed to broadcast addresses.
Unicast bytes	The total amount of memory (in bytes) used by unicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Multicast bytes	The total amount of memory (in bytes) used by multicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Broadcast bytes	The total amount of memory (in bytes) used by broadcast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Alignment errors	The total number of frames received on an interface that have alignment errors.
FCS errors	The total number of frames received on an interface that have a valid length (in bytes) but do not have the correct FCS values.
Oversize frames	The number of frames received on an interface that are larger than the maximum allowed frame size.
Undersize frames	The number of frames received on an interface that are smaller than 64 bytes.
Collision fragments	The number of collision fragments received on an interface.
Minimum size frames	The total number of frames that are the minimum frame size.
65 to 127 byte frames	The total number of frames that are from 65 to 127 bytes.
128 to 255 byte frames	The total number of frames that are from 128 to 255 bytes.
256 to 511 byte frames	The total number of frames that are from 256 to 511 bytes.
512 to 1023 byte frames	The total number of frames that are from 512 to 1023 bytes.
1024 to 1518 byte frames	The total number of frames that are from 1024 to 1518 bytes.
Overrun frames	The total number of overrun frames received on an interface.
Pause frames	The number of pause frames received on an interface.
Symbol error frames	The number of frames received on an interface that have symbol errors.
Invalid frames, too large	The number of frames received that were larger than maximum allowed MTU[2] size (including the FCS bits and excluding the frame header) and that have either an FCS error or an alignment error.
Valid frames, too large	The number of frames received on an interface that are larger than the maximum allowed frame size.
Invalid frames, too small	The number of frames received that are smaller than 64 bytes (including the FCS bits and excluding the frame header) and that have either an FCS error or an alignment error.
Valid frames, too small	The number of frames received on an interface that are smaller than 64 bytes (or 68 bytes for VLAN-tagged frames) and that have valid FCS values. The frame size includes the FCS bits but excludes the frame header bits.
Too old frames	The number of frames dropped on the ingress port because the packet aged out.
Valid oversize frames	The number of frames received on an interface that are larger than the maximum allowed frame size and have valid FCS values. The frame size includes the FCS value but does not include the VLAN tag.

Table 3-9 Receive Field Descriptions (continued)

Field	Description
System FCS error frames	The total number of frames received on an interface that have a valid length (in bytes) but that do not have the correct FCS values.
RxPortFifoFull drop frames	The total number of frames received on an interface that are dropped because the ingress queue is full.

1. FCS = frame check sequence
2. MTU = maximum transmission unit

This is an example of output from the **show controllers ethernet-controller phy** command for a specific interface.

```
Switch# show controllers ethernet-controller gigabitethernet0/1 phy

GigabitEthernet0/1 (port-number: 1)
------------------------------------------------------------

General SFP Information
-----------------------------------------------
Identifier            :   0x03
Connector             :   0x00
Transceiver           :   0x00 0x00 0x00 0x08 0x00 0x00 0x00 0x00
Encoding              :   0x01
BR_Nominal            :   0x0D
Vendor Name           :   CISCO-METHODE
Vendor Part Number    :   SP7041
Vendor Revision       :   0x44 0x20 0x20 0x20
Vendor Serial Number  :   00000MTC111701L3
-----------------------------------------------

EEPROM PAGE A0

-----------------------------------------------
000:  03 04 00 00 00 00 08 00 00 00
010:  00 01 0D 00 00 00 00 00 64 00
020:  43 49 53 43 4F 2D 4D 45 54 48
030:  4F 44 45 20 20 20 01 00 00 00
040:  53 50 37 30 34 31 20 20 20 20
```

Related Commands

Command	Description
show controllers cpu-interface	Displays the state of the CPU network ASIC and send and receive statistics for packets reaching the CPU.

show controllers utilization

To display bandwidth utilization on the switch or specific ports, use the **show controllers utilization** command in user EXEC mode.

show controllers [*interface-id*] **utilization** [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) ID of the switch interface.
| begin	(Optional) Display begins with the line that matches the specified *expression*.
| exclude	(Optional) Display excludes lines that match the specified *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show controllers utilization** command.

```
Switch> show controllers utilization
Port       Receive Utilization  Transmit Utilization
Gi0/1              0                    0
Gi0/2              0                    0
Gi0/3              0                    0
Gi0/4              0                    0
Gi0/5              0                    0
Gi0/6              0                    0
Gi0/7              0                    0
Gi0/8              0                    0
Gi0/9              0                    0
Gi0/10             0                    0
Gi0/11             0                    0
Gi0/12             0                    0
Gi0/13             0                    0
Gi0/14             0                    0
Gi0/15             0                    0
Gi0/16             0                    0
Gi0/17             0                    0
Gi0/18             0                    0
Gi0/19             0                    0
Gi0/20             0                    0
Gi0/21             0                    0
Gi0/22             0                    0
Gi0/23             0                    0
```

```
Gi0/24              0                    0
Te0/1               0                    0
Te0/2               0                    0

Total Ports : 26
Switch Receive Bandwidth Percentage Utilization  : 0
Switch Transmit Bandwidth Percentage Utilization : 0

Switch Fabric Percentage Utilization : 0
```

This is an example of output from the **show controllers utilization** command on a specific port:

```
Switch> show controllers gigabitethernet0/1 utilization
Receive Bandwidth Percentage Utilization   : 0
Transmit Bandwidth Percentage Utilization  : 0
```

Table 3-10 show controllers utilization Field Descriptions

Field	Description
Receive Bandwidth Percentage Utilization	Displays the received bandwidth usage of the switch, which is the sum of the received traffic on all the ports divided by the switch receive capacity.
Transmit Bandwidth Percentage Utilization	Displays the transmitted bandwidth usage of the switch, which is the sum of the transmitted traffic on all the ports divided it by the switch transmit capacity.
Fabric Percentage Utilization	Displays the average of the transmitted and received bandwidth usage of the switch.

Related Commands

Command	Description
show controllers ethernet-controller	Displays the interface internal registers.

show diagnostic

To display the online diagnostic test results and the supported test suites, use the **show diagnostic** command in user EXEC mode.

show diagnostic content [**|** {**begin | exclude | include**} *expression*]

show diagnostic detail [**|** {**begin | exclude | include**} *expression*]

show diagnostic post [**|**{**begin | exclude | include**} *expression*]

show diagnostic result [**test** {*name* **|** *test-id* **|** *test-id-range* **| all**}] [**detail**] [**|** {**begin | exclude | include**} *expression*]

show diagnostic schedule [**|** {**begin | exclude | include**} *expression*]

show diagnostic status [**|** {**begin | exclude | include**} *expression*]

Syntax Description

content	Displays test information including the test ID, the test attributes, and the supported coverage test levels for specific tests and for switches.
detail	Displays detailed test results.
post	Displays the power-on self-test (POST) results.
result	Displays the diagnostic test results.
test	(Optional) Specifies the test results to display: • *name*—Enter the name of the diagnostic test to display results only for this test. • *test-id*—Enter the test ID number to display results only for this test. The test ID can be from 1 to 6. • *test-id-range*—Enter the range of test ID numbers to display results only for these tests. • **all**—Enter this keyword to display results for all the tests.
detail	(Optional) Displays the detailed test results.
schedule	Displays the scheduled diagnostic tests.
status	Display the running diagnostic tests.
| begin	(Optional) Display begins with the line that matches the expression.
| exclude	(Optional) Display excludes lines that match the expression.
| include	(Optional) Display includes lines that match the specified expression.
expression	Expression in the output to use as a reference point.

Defaults

This command has no default setting.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **show diagnostic post** command output is the same as the **show post** command output.

The **show diagnostic result** [**detail**] command output is the same as the **show diagnostic switch** [**detail**] command output.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This example shows how to display the diagnostic test IDs and attributes.

```
Switch> show diagnostic content

  Diagnostics test suite attributes:
      B/* - Basic ondemand test / NA
    P/V/* - Per port test / Per device test / NA
    D/N/* - Disruptive test / Non-disruptive test / NA
      S/* - Only applicable to standby unit / NA
      R/* - Switch will reload after test list completion / NA
      P/* - will partition stack / NA

  ID   Test Name                          Attributes
  ==== ================================== ============
    1) TestPortAsicMem -----------------> B*D*R*
    2) TestPortAsicCam -----------------> B*D*R*
    3) TestPortAsicLoopback ------------> B*D*R*
    4) TestPortLoopback ----------------> B*D*R*
    5) TestFpga ------------------------> B*D*R*
```

This example shows how to display the diagnostic test results for a switch. You can also use the **show diagnostic switch** command to display these results.

```
Switch> show diagnostic result
:   SerialNo : FHH1329P00B

  Overall diagnostic result: UNTESTED

  Test results: (. = Pass, F = Fail, U = Untested)

    1) TestPortAsicMem -----------------> U
    2) TestPortAsicCam -----------------> U
    3) TestPortAsicLoopback ------------> U
    4) TestPortLoopback ----------------> U
    5) TestFpga ------------------------> U
```

This example shows how to display the running tests in a switch:

```
Switch> show diagnostic status
<BU> - Bootup Diagnostics, <HM> - Health Monitoring Diagnostics,
<OD> - OnDemand Diagnostics, <SCH> - Scheduled Diagnostics

====== ================================= ================================ ======
Card   Description                       Current Running Test             Run by
------ --------------------------------- -------------------------------- ------
sw     FHH1329P00B                       N/A                              N/A

====== ================================= ================================ ======
```

This example shows how to display the online diagnostic test schedule for a switch:

```
Switch> show diagnostic schedule
Current Time = 14:39:49 PST Tue Jul 5 2005
Diagnostic for Switch 1:
Schedule #1:
To be run daily 12:00
Test ID(s) to be executed: 1.
```

This example shows how to display the detailed results for a switch. You can also use the **show diagnostic result test all detail** command to display these results.

```
Switch> show diagnostic result test all detail

Test results: (. = Pass, F = Fail, U = Untested)

_____________________________________________________________________________

  1) TestPortAsicMem ------------------> U

        Error code -------------------> 0 (DIAG_SUCCESS)
        Total run count --------------> 0
        Last test execution time ----> n/a
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> n/a
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

  2) TestPortAsicCam ------------------> U

        Error code -------------------> 0 (DIAG_SUCCESS)
        Total run count --------------> 0
        Last test execution time ----> n/a
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> n/a
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

  3) TestPortAsicLoopback -------------> U

        Error code -------------------> 0 (DIAG_SUCCESS)
        Total run count --------------> 0
        Last test execution time ----> n/a
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> n/a
        Total failure count ---------> 0
        Consecutive failure count ---> 0
_____________________________________________________________________________

  4) TestPortLoopback -----------------> U

        Error code -------------------> 0 (DIAG_SUCCESS)
        Total run count --------------> 0
        Last test execution time ----> n/a
        First test failure time -----> n/a
        Last test failure time ------> n/a
        Last test pass time ---------> n/a
        Total failure count ---------> 0
        Consecutive failure count ---> 0
```

```
5) TestFpga ------------------------> U

      Error code -------------------> 0 (DIAG_SUCCESS)
      Total run count --------------> 0
      Last test execution time ----> n/a
      First test failure time -----> n/a
      Last test failure time ------> n/a
      Last test pass time ---------> n/a
      Total failure count ---------> 0
      Consecutive failure count ---> 0
```

Related Commands

Command	Description
diagnostic monitor	Configures the health-monitoring diagnostic test.
diagnostic schedule test	Sets the scheduling of test-based online diagnostic testing.
diagnostic start test	Starts the online diagnostic test.

show env

To display alarm contact, fan, temperature, and power information for the switch, use the **show env** command in user EXEC mode.

show env {**alarm-contact** | **all** | **fan** | **power**| **temperature** [**status**]} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

alarm-contact	Displays alarm contact status.
all	Displays fan, temperature, power supply, and alarm status.
fan	Displays the switch fan status, including the power-supply fan.
power	Displays the switch power-supply status.
temperature	Displays the switch temperature status as GREEN or RED.
status	(Optional) Shows more detailed temperature status, including the temperature value, state (green, yellow, or red), and the yellow and red threshold values.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can use the **show env temperature status** command to display the switch temperature status. The command output shows the temperature state as green or red and shows the shutdown and alert thresholds. The output from the **show env all** command also includes this information.

For more information about the threshold levels, see the software configuration guide for this release.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show env alarm-contact** command:

```
Switch# show env alarm-contact
ALARM CONTACT 1
   Status:      not asserted
   Description: external alarm contact 1
   Severity:    minor
   Trigger:     closed
ALARM CONTACT 2
   Status:      not asserted
   Description: external alarm contact 2
   Severity:    minor
   Trigger:     closed
ALARM CONTACT 3
   Status:      not asserted
   Description: external alarm contact 3
   Severity:    minor
   Trigger:     closed
ALARM CONTACT 4
   Status:      not asserted
   Description: external alarm contact 4
   Severity:    minor
```

This is an example of output from the **show env all** command:

```
Switch> show env all
FAN in PS-1 is OK
FAN in FANTRAY-2 is OK
SYSTEM TEMPERATURE is GREEN
SYSTEM Temperature Value: 35.5 Degree Celsius
SYSTEM Temperature State: GREEN
SYSTEM Low Temperature Alert Threshold: 0.0 Degree Celsius
SYSTEM Low Temperature Shutdown Threshold: -20.0 Degree Celsius
SYSTEM High Temperature Alert Threshold: 58.0 Degree Celsius
SYSTEM High Temperature Shutdown Threshold: 80.0 Degree Celsius
POWER SUPPLY 1 Temperature Value: 32.7500 Degree Celsius
POWER SUPPLY 1 Temperature Alert Threshold: 85.0000 Degree Celsius
POWER SUPPLY 1 Temperature Shutdown Threshold: 110.0000 Degree Celsius
FAN TRAY 2: No Temperature Information Provided
POWER SUPPLY 1 is AC OK
POWER SUPPLY 2 is Fan Tray OK

ALARM CONTACT 1 is not asserted
ALARM CONTACT 2 is not asserted
ALARM CONTACT 3 is not asserted
ALARM CONTACT 4 is not asserted
```

This is an example of output from the **show env fan** command for the Cisco ME 3400G-12CS switch:

```
Switch> show env fan
FAN in PS-1 is OK
FAN in FANTRAY-2 is OK
```

This is an example of output from the **show env power** command for the Cisco ME 3400G-12CS switch:

```
Switch> show env power
POWER SUPPLY 1 is AC OK
   AC Input  : OK
   Output    : OK
   Fan       : OK
POWER SUPPLY 2 is Fan Tray OK
   Fan       : OK
```

These are examples of output from the **show env temperature** and **show env temperature status** commands:

```
Switch> show env temperature
SYSTEM TEMPERATURE is GREEN

Switch> show env temperature status
SYSTEM Temperature Value: 35.5 Degree Celsius
SYSTEM Temperature State: GREEN
SYSTEM Low Temperature Alert Threshold: 0.0 Degree Celsius
SYSTEM Low Temperature Shutdown Threshold: -20.0 Degree Celsius
SYSTEM High Temperature Alert Threshold: 58.0 Degree Celsius
SYSTEM High Temperature Shutdown Threshold: 80.0 Degree Celsius
POWER SUPPLY 1 Temperature Value: 32.7500 Degree Celsius
POWER SUPPLY 1 Temperature Alert Threshold: 85.0000 Degree Celsius
POWER SUPPLY 1 Temperature Shutdown Threshold: 110.0000 Degree Celsius
FAN TRAY 2: No Temperature Information Provided
```

Related Commands

Command	Description
system env temperature threshold alert	Configures the system temperature thresholds.
alarm-contact	Configures alarm contacts.

show errdisable detect

To display error-disable detection status, use the **show errdisable detect** command in user EXEC mode.

show errdisable detect [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The `Mode` column shows the shutdown mode that was configured for the error-disabled reason:

- port—The physical port is error disabled if a violation occurs.
- vlan—The virtual port is disabled if a violation occurs.
- port/vlan—Some ports are configured for physical port disable, and others are configured for virtual port disable. Enter the **show running config** privileged EXEC command to see the configuration for each port.

A displayed `gbic-invalid` error in the `Reason` column refers to an invalid small form-factor pluggable (SFP) interface.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show errdisable detect** command:

```
Switch> show errdisable detect
ErrDisable Reason            Detection    Mode
-----------------            ---------    ----
arp-inspection               Enabled      port
bpduguard                    Enabled      port
channel-misconfig (STP)      Enabled      port
community-limit              Enabled      port
dhcp-rate-limit              Enabled      port
dtp-flap                     Enabled      port
gbic-invalid                 Enabled      port
invalid-policy               Enabled      port
link-flap                    Enabled      port
link-monitor-failure         Enabled      port
loopback                     Enabled      port
lsgroup                      Enabled      port
oam-remote-failure           Enabled      port
```

```
mac-limit                   Enabled      port
pagp-flap                   Enabled      port
port-mode-failure           Enabled      port
pppoe-ia-rate-limit         Enabled      port
psecure-violation           Enabled      port
security-violation          Enabled      port
sfp-config-mismatch         Enabled      port
storm-control               Enabled      port
udld                        Enabled      port
vmps                        Enabled      port
```

Note Though visible in the output, the dtp-flap and arp-inspection fields are not valid.

Related Commands

Command	Description
errdisable detect cause	Enables error-disable detection for a specific cause or all causes.
show errdisable flap-values	Displays error condition recognition information.
show errdisable recovery	Displays error-disable recovery timer information.
show interfaces status	Displays interface status or a list of interfaces in an error-disabled state.

show errdisable flap-values

To display conditions that cause an error to be recognized for a cause, use the **show errdisable flap-values** command in user EXEC mode.

show errdisable flap-values [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The *Flaps* column in the display shows how many changes to the state within the specified time interval will cause an error to be detected and a port to be disabled. For example, the display shows that an error will be assumed and the port shut down if three Dynamic Trunking Protocol (DTP)-state (port mode access/trunk) or Port Aggregation Protocol (PAgP) flap changes occur during a 30-second interval, or if 5 link-state (link up/down) changes occur during a 10-second interval.

```
ErrDisable Reason    Flaps    Time (sec)
-----------------    ------   ----------
pagp-flap              3       30
dtp-flap               3       30
link-flap              5       10
```

Note Although visible in the output display, the switch does not support DTP.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show errdisable flap-values** command:

```
Switch> show errdisable flap-values
ErrDisable Reason    Flaps    Time (sec)
-----------------    ------   ----------
pagp-flap              3       30
dtp-flap               3       30
link-flap              5       10
```

Related Commands

Command	Description
errdisable detect cause	Enables error-disable detection for a specific cause or all causes.
show errdisable detect	Displays error-disable detection status.
show errdisable recovery	Displays error-disable recovery timer information.
show interfaces status	Displays interface status or a list of interfaces in error-disabled state.

show errdisable recovery

To display the error-disable recovery timer information, use the **show errdisable recovery** command in user EXEC mode.

show errdisable recovery [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

A *gbic-invalid error-disable* reason refers to an invalid small form-factor pluggable (SFP) module interface.

Examples

This is an example of output from the **show errdisable recovery** command:

```
Switch> show errdisable recovery
ErrDisable Reason            Timer Status
-----------------            --------------
arp-inspection               Disabled
bpduguard                    Disabled
channel-misconfig (STP)      Disabled
dhcp-rate-limit              Disabled
dtp-flap                     Disabled
gbic-invalid                 Disabled
link-flap                    Disabled
mac-limit                    Disabled
link-monitor-failure         Disabled
loopback                     Disabled
oam-remote-failure           Disabled
pagp-flap                    Disabled
port-mode-failure            Disabled
pppoe-ia-rate-limit          Disabled
psecure-violation            Disabled
security-violation           Disabled
sfp-config-mismatch          Disabled
storm-control                Disabled
udld                         Disabled
vmps                         Disabled
```

```
Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:
Interface    Errdisable reason    Time left(sec)
---------    -----------------    --------------
Gi0/2        link-flap             279
```

Note Though visible in the output, the unicast-flood and DTP fields are not valid.

Related Commands

Command	Description
errdisable recovery	Configures the recover mechanism variables.
show errdisable detect	Displays error-disabled detection status.
show errdisable flap-values	Displays error condition recognition information.
show interfaces status	Displays interface status or a list of interfaces in error-disabled state.

show etherchannel

To display EtherChannel information for a channel, use the **show etherchannel** command in user EXEC mode.

show etherchannel [*channel-group-number* {**detail | port | port-channel | protocol | summary**}] {**detail | load-balance | port | port-channel | protocol | summary**} [| {**begin | exclude | include**} *expression*]

Syntax Description

channel-group-number	(Optional) Number of the channel group. The range is 1 to 26.
detail	Displays detailed EtherChannel information.
load-balance	Displays the load-balance or frame-distribution scheme among ports in the port channel.
port	Displays EtherChannel port information.
port-channel	Displays port-channel information.
protocol	Displays the protocol that is being used in the EtherChannel.
summary	Displays a one-line summary per channel-group.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If you do not specify a *channel-group*, all channel groups are displayed.

In the output, the Passive port list field is displayed only for Layer 3 port channels. This field means that the physical port, which is still not up, is configured to be in the channel group (and indirectly is in the only port channel in the channel group).

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show etherchannel 1 detail** command:

```
Switch> show etherchannel 1 detail
Group state = L2
Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP
               Ports in the group:
               -------------------
Port: Gi0/1
------------

Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = Active      Gcchange = -
Port-channel  = Po1         GC   =   -         Pseudo port-channel = Po1
Port index    = 0           Load = 0x00        Protocol =   LACP

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDU
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port     Port
Port      Flags   State     Priority      Key       Key     Number   State
Gi0/1     SA      bndl      32768         0x0       0x1     0x0      0x3D

Age of the port in the current state: 01d:20h:06m:04s

               Port-channels in the group:
               ----------------------

Port-channel: Po1    (Primary Aggregator)
------------

Age of the Port-channel   = 01d:20h:20m:26s
Logical slot/port   = 10/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
0     00     Gi0/1    Active          0
  0     00     Gi0/2    Active          0

Time since last port bundled:    01d:20h:20m:20s    Gi0/2
```

This is an example of output from the **show etherchannel 1 summary** command:

```
Switch> show etherchannel 1 summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        u - unsuitable for bundling
        U - in use      f - failed to allocate aggregator
        d - default port

Number of channel-groups in use: 1
Number of aggregators:           1
```

```
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
1      Po1(SU)         LACP      Gi0/1(P)    Gi0/2(P)
```

This is an example of output from the **show etherchannel 1 port-channel** command:

```
Switch> show etherchannel 1 port-channel
                Port-channels in the group:
                ----------------------
Port-channel: Po1    (Primary Aggregator)

------------

Age of the Port-channel   = 01d:20h:24m:50s
Logical slot/port   = 10/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi0/1    Active          0
  0     00     Gi0/2    Active          0

Time since last port bundled:    01d:20h:24m:44s    Gi0/2
```

This is an example of output from **show etherchannel protocol** command:

```
Switch# show etherchannel protocol
                Channel-group listing:
                ----------------------
Group: 1
----------
Protocol:  LACP

Group: 2
----------
Protocol:  PAgP
```

Related Commands

Command	Description
channel-group	Assigns an Ethernet port to an EtherChannel group.
channel-protocol	Restricts the protocol used on a port to manage channeling.
interface port-channel	Accesses or creates the port channel.

show ethernet service evc

To display information about Ethernet virtual connection (EVC) customer-service instances, use the **show ethernet service evc** command in privileged EXEC mode.

show ethernet service evc [**id** *evc-id* | **interface** *interface-id*] [**detail**] [**summary**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

id *evc-id*	(Optional) Displays EVC information for the specified service. The EVC identifier can be a string of from 1 to 100 characters.
interface *interface-id*	(Optional) Displays EVC information for the specified interface.
detail	(Optional) Displays detailed information about EVC service or the specified EVC ID or interface.
summary	(Optional) Displays summary of information for EVC service or the specified EVC interface.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show ethernet service evc** command:

```
Switch# show ethernet service evc
Identifier                      Type  Act-UNI-cnt Status
BLUE                            P-P       2       Active
PINK                            MP-MP     2       PartiallyActive
PURPLE                          P-P       2       Active
BROWN                           MP-MP     2       Active
GREEN                           P-P       3       Active
YELLOW                          MP-MP     2       PartiallyActive
BANANAS                         P-P       0       InActive
TEST2                           P-P       0       NotDefined
ORANGE                          P-P       2       Active
TEAL                            P-P       0       InActive
```

Related Commands

Command	Description
ethernet evc *evc-id*	Defines an EVC and enters EVC configuration mode.

show flowcontrol

To display the flow control status and statistics, use the **show flowcontrol** command in user EXEC mode.

show flowcontrol [**interface** *interface-id* | **module** *number*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface *interface-id*	(Optional) Displays the flow control status and statistics for a specific interface.
module *number*	(Optional) Displays the flow control status and statistics for all interfaces on the switch. The only valid module number is 1. This option is not available if you have entered a specific interface ID.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use this command to display the flow control status and statistics on the switch or for a specific interface.

Use the **show flowcontrol** command to display information about all the switch interfaces. The output from the **show flowcontrol** command is the same as the output from the **show flowcontrol module** *number* command.

Use the **show flowcontrol interface** *interface-id* command to display information about a specific interface.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show flowcontrol** command.

```
Switch> show flowcontrol
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
           admin    oper     admin    oper
---------  -------- -------- -------- --------    ------- -------
Gi0/1      Unsupp.  Unsupp.  off      off         0       0
Gi0/2      desired  off      off      off         0       0
Gi0/3      desired  off      off      off         0       0
<output truncated>
```

This is an example of output from the **show flowcontrol interface** *interface-id* command:

```
Switch> show flowcontrol interface gigabitethernet0/2
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
           admin    oper     admin    oper
---------  -------- -------- -------- --------    ------- -------
Gi0/2      desired  off      off      off         0       0
```

Related Commands

Command	Description
flowcontrol	Sets the receive flow-control state for an interface.

show interfaces

To display the administrative and operational status of all interfaces or a specified interface, use the **show interfaces** command in privileged EXEC mode.

show interfaces [*interface-id* | **vlan** *vlan-id*] [**accounting** | **capabilities** [**module** *number*] | **counters** | **dampening** | **debounce** [**module**] | **description** | **etherchannel** | **flowcontrol** | **rep** | **stats** | **status** [**err-disabled**] | **switchport** [**backup** | **module** *number*] | **transceivers** [**properties** | **detail**] [**module** *number*] | **trunk**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) Valid interfaces include physical ports (including type, module, and port number) and port channels. The port-channel range is 1 to 48.
vlan *vlan-id*	(Optional) VLAN identification. The range is 1 to 4094.
accounting	(Optional) Displays accounting information on the interface, including active protocols and input and output packets and octets.
capabilities	(Optional) Displays the capabilities of all interfaces or the specified interface, including the features and options that you can configure on the interface. Though visible in the command line help, this option is not available for VLAN IDs.
module *number*	(Optional) Displays **capabilities**, **switchport** configuration, or **transceiver** characteristics (depending on preceding keyword) of all interfaces on the switch. The only valid module number is 1. This option is not available if you have entered a specific interface ID.
counters	(Optional) See the **show interfaces counters** command.
dampening	(Optional) Displays interface dampening information.
debounce [**module**]	(Optional) Displays interface debounce time information.
description	(Optional) Displays the administrative status and description set for an interface.
etherchannel	(Optional) Displays interface EtherChannel information.
fcpa	(Optional) Displays fiber channel information
flowcontrol	(Optional) Displays interface flowcontrol information
mpls-exp	(Optional) Display interface MPLS experimental accounting information.
rep	(Optional) See the **show interfaces rep** command.
stats	(Optional) Displays the input and output packets by switching path for the interface.
status	(Optional) Displays the status of the interface. A status of *unsupported* in the Type field means that a non-Cisco small form-factor pluggable (SFP) module is inserted in the module slot.
err-disabled	(Optional) Displays interfaces in error-disabled state.
switchport	(Optional) Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
backup	(Optional) Displays the backup interface configuration.
module	(Optional) Limits the display to interfaces on a module
transceivers	(Optional) See the **show interfaces transceiver** command.
trunk	Displays interface trunk information. If you do not specify an interface, only information for active trunking ports appears.

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help strings, the **crb**, **private-vlan mapping**, **pruning random-detect**, and **rate-limit** keywords are not supported.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **show interfaces capabilities** command with different keywords has these results:

- Use the **show interface capabilities module 1** to display the capabilities of all interfaces on the switch. Entering any other number is invalid.
- Use the **show interfaces** *interface-id* **capabilities** to display the capabilities of the specified interface.
- Use the **show interfaces capabilities** (with no module number or interface ID) to display the capabilities of all interfaces on the switch.
- Use the **show interface switchport module 1** to display the switch port characteristics of all interfaces on the switch. Entering any other number is invalid.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show interfaces** command for an interface:

```
Switch# show interfaces gigabitethernet0/1
GigabitEthernet0/1 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 0023.eb17.c781 (bia 0023.eb17.c781)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Full-duplex, 1000Mb/s, link type is auto, media type is 10/100/1000BaseTX SFP
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:14, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     28980 packets input, 2882755 bytes, 0 no buffer
```

```
     Received 16517 broadcasts (15276 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 15276 multicast, 0 pause input
     0 input packets with dribble condition detected
     4186 packets output, 1322776 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

This is an example of output from the **show interfaces accounting** command.

```
Switch# show interfaces accounting
VGigabitEthernet0
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                   Other       8468     810077          1         60
                      IP    3156345  260882105    5133740  504298864
           Spanning Tree      62855    3771300          0          0
                     ARP      64072    3906250         38       2280
                     CDP       2110     827120       2106     720252
Interface Vlan1 is disabled

GigabitEthernet0/1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                   Other          0          0       4188    1306656
                     CDP          0          0       2129     766440
GigabitEthernet0/2
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                   Other          0          0       4187    1306344
                     CDP          0          0       2129     766440
GigabitEthernet0/3
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                   Other          0          0       4211    1313832
                     CDP          0          0       2106     758160
GigabitEthernet0/4
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                   Other          0          0       4211    1313832
                      IP          0          0          6        360
           Spanning Tree          0          0      61843    3710580
                     CDP       2104     864744       2106     758160
GigabitEthernet0/5
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                   Other          0          0       4188    1306656
           Spanning Tree         23       1380      61547    3692820
                     CDP       2139     796595       2130     766800
GigabitEthernet0/6
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                   Other          0          0       3435    1044240
                    CLNS          0          0        144     218016
                     ARP          0          0          3        180
                     CDP       1740     648394       1733     596712
GigabitEthernet0/7
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
GigabitEthernet0/8
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
GigabitEthernet0/9
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
<output truncated>
```

This is an example of output from the **show interfaces capabilities** command for an interface.

```
Switch# show interfaces gigabitethernet0/2 capabilities
GigabitEthernet0/2
Model:                 ME-3800X-24FS-M
 Type:                  10/100/1000BaseTX SFP
 Speed:                 10,100,1000,auto
 Duplex:                half,full,auto
 Trunk encap. type:     802.1Q
 Trunk mode:            on,off,desirable,nonegotiate
 Channel:               yes
 Broadcast suppression: percentage(0-100)
 Flowcontrol:           rx-(off,on,desired),tx-(none)
 Fast Start:            yes
 QoS scheduling:        Rx-no ingress scheduling
                        tx-three levels of hierarchy and 2 level scheduling
 CoS rewrite:           yes
 ToS rewrite:           yes
 UDLD:                  yes
 Inline power:          no
 SPAN:                  no
 PortSecure:            no
 Dot1x:                 no
```

This is an example of output from the **show interfaces** *interface* **description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command.

```
Switch# show interfaces gigabitethernet0/2 description
Interface Status         Protocol Description
Gi0/2       up             down     Connects to Marketing
```

This is an example of output from the **show interfaces etherchannel** command when port channels are configured on the switch:

```
Switch# show interfaces etherchannel
----
Port-channel1:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/1           Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse

Port-channel2:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/2           Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse

Port-channel3:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/3           Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse
```

This is an example of output from the **show interfaces stats** command for a specified VLAN interface.

```
Switch# show interfaces vlan 1 stats
Switching path    Pkts In   Chars In   Pkts Out  Chars Out
        Processor    1165354  136205310     570800   91731594
      Route cache          0          0          0          0
            Total    1165354  136205310     570800   91731594
```

This is an example of partial output from the **show interfaces status** command. It displays the status of all interfaces.

```
Switch# show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/1                        connected    trunk      a-full a-1000 10/100/1000Ba
seTX SFP
Gi0/2                        connected    trunk      a-full a-1000 10/100/1000Ba
seTX SFP
Gi0/3                        connected    trunk      a-full a-1000 10/100/1000Ba
seTX SFP
Gi0/4                        connected    1          a-full a-1000 10/100/1000Ba
seTX SFP
Gi0/5                        connected    1          a-full a-1000 10/100/1000Ba
seTX SFP
Gi0/6                        connected    routed     a-full a-1000 10/100/1000Ba
seTX SFP
Gi0/7                        notconnect   1            auto   auto Not Present
Gi0/8                        notconnect   1            auto   auto Not Present
Gi0/9                        notconnect   trunk        auto   auto Not Present
Gi0/10                       notconnect   1            auto   auto Not Present
Gi0/11    testwhelshdevice   connected    1          a-full a-1000 10/100/1000Ba
seTX SFP
Gi0/12                       notconnect   1            auto   auto Not Present
Gi0/13                       connected    trunk      a-full    100 10/100/1000Ba
seTX SFP
Gi0/14                       connected    1          a-full a-1000 10/100/1000Ba
seTX SFP

Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/15                       connected    1          a-full a-1000 10/100/1000Ba
seTX SFP
Gi0/16                       connected    1          a-full a-1000 10/100/1000Ba
seTX SFP
Gi0/17                       notconnect   1            auto   auto Not Present
Gi0/18                       notconnect   1            auto   auto Not Present
Gi0/19                       notconnect   1            auto   auto Not Present
Gi0/20                       notconnect   1            auto   auto Not Present
Gi0/21                       notconnect   1            auto   auto Not Present
Gi0/22                       notconnect   1            auto   auto Not Present
Gi0/23                       notconnect   1            auto   auto Not Present
Gi0/24                       notconnect   1            auto   auto Not Present
Te0/1                        disabled     1            full    10G Not Present
Te0/2                        disabled     1            full    10G SFP-10GBase-C
UxM
Port      Name               Status       Vlan       Duplex  Speed Type
Gi0                          connected    routed     a-full  a-100 10/100/1000Ba
seTX
```

These are examples of output from the **show interfaces status** command for a specific interface when private VLANs are configured. Port 22 is configured as a private-VLAN host port. It is associated with primary VLAN 20 and secondary VLAN 25.

```
Switch# show interfaces gigabitethernet0/22 status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/2                        connected    trunk      a-full a-1000 10/100/1000Ba
seTX SFP
```

This is an example of output from the **show interfaces status err-disabled** command for an interface:

```
Switch# show interfaces gigabitethernet0/2 status err-disabled

Port      Name               Status       Reason               Err-disabled Vlans
Gi0/2                        connected    elmi evc down        1,200
```

This is an example of output from the **show interfaces switchport** command for a single port. Table 2-12 describes the fields in the display.

Note Private VLAN trunks are not supported in this release, so those fields are not applicable.

```
Switch# show interfaces gigabitethernet0/8 switchport
Name: Gi0/8
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Table 3-11 show interfaces switchport Field Descriptions

Field	Description
Name	Displays the port name.
Switchport	Displays the administrative and operational status of the port. In this display, the port is in switchport mode.
Administrative Mode Operational Mode	Displays the administrative and operational modes.
Administrative Trunking Encapsulation Negotiation of Trunking	Displays the administrative and operational encapsulation method and whether trunking negotiation is enabled.
Access Mode VLAN	Displays the VLAN ID to which the port is configured.
Trunking Native Mode VLAN	Lists the VLAN ID of the trunk that is in native mode.
Administrative Native VLAN tagging	Displays whether or not VLAN tagging is enabled.

Table 3-11 show interfaces switchport Field Descriptions (continued)

Field	Description
Administrative private-vlan host-association	Displays the administrative VLAN association for private-VLAN host ports.
Administrative private-vlan mapping	Displays the administrative VLAN mapping for private-VLAN promiscuous ports.
Operational private-vlan	Displays the operational private-VLAN status.
Trunking VLANs enabled	Lists the active VLANs on the trunk.
Capture VLANs allowed	Lists the allowed VLANs on the trunk.
Unknown unicast blocked Unknown multicast blocked	Displays whether or not unknown multicast and unknown unicast traffic is blocked on the interface.

This is an example of output from the **show interfaces** *interface-id* **trunk** command. It displays trunking information for the port.

```
Switch# show interfaces gigabitethernet0/1 trunk
Port          Mode         Encapsulation  Status        Native vlan
Gi0/1         auto         negotiate      trunking      1

Port          Vlans allowed on trunk
Gi0/1         1-4094

Port          Vlans allowed and active in management domain
Gi0/1         1-4

Port          Vlans in spanning tree forwarding state and not pruned
Gi0/1         1-4
```

Related Commands

Command	Description
switchport access vlan	Configures a port as a static-access or a dynamic-access port.
switchport block	Blocks unknown unicast or multicast traffic on an interface.
switchport mode	Configures the VLAN membership mode of a port.

show interfaces counters

To display various counters for the switch or for a specific interface, use the **show interfaces counters** command in privileged EXEC mode.

show interfaces [*interface-id* | **vlan** *vlan-id*] **counters** [**errors** | **trunk**] [**module** *switch- number*] | **etherchannel** | **protocol status**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) ID of the physical interface, including type, module, and port number.
errors	(Optional) Displays error counters.
trunk	(Optional) Displays trunk counters.
module *switch- number*	(Optional) Displays counters for the specified switch number. The only available value is 1.
etherchannel	(Optional) Displays EtherChannel counters, including octets, broadcast packets, multicast packets, and unicast packets received and sent.
protocol status	(Optional) Displays status of protocols enabled on interfaces.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help string, the **vlan** *vlan-id* keyword is not supported.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If you do not enter any keywords, all counters for all interfaces are included.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of partial output from the **show interfaces counters** command. It displays all counters for the switch.

```
Switch# show interfaces counters
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi0/1            2895390          12518          15343           1247
Gi0/2            1609255          12517           2147              0
Gi0/3            3524654          12617          23846              1
Gi0/4            3391800          12617          21768              1
Gi0/5            1610919          12516           2174              0
Gi0/6            1315586          10269           1748              0
Gi0/7                  0              0              0              0
Gi0/8                  0              0              0              0
Gi0/9                  0              0              0              0
Gi0/10                 0              0              0              0
Gi0/11           1610151          12517           2161              0
Gi0/12                 0              0              0              0
Gi0/13                 0              0              0              0
Gi0/14                 0              0              0              0
Gi0/15                 0              0              0              0
Gi0/16                 0              0              0              0
Gi0/17                 0              0              0              0
Gi0/18                 0              0              0              0
Gi0/19                 0              0              0              0
Gi0/20                 0              0              0              0
Gi0/21                 0              0              0              0

<output truncated>
```

This is an example of partial output from the **show interfaces counters protocol status** command for all interfaces.

```
Switch# show interfaces counters protocol status
Protocols allocated:
 GigabitEthernet0: Other, IP, Spanning Tree, ARP, CDP
 Vlan1: Other, IP
 GigabitEthernet0/1: Other, IP, CDP
 GigabitEthernet0/2: Other, IP, CDP
 GigabitEthernet0/3: Other, IP, CDP
 GigabitEthernet0/4: Other, IP, Spanning Tree, CDP
 GigabitEthernet0/5: Other, IP, Spanning Tree, CDP
 GigabitEthernet0/6: Other, IP, CLNS, ARP, CDP
 GigabitEthernet0/7: Other, IP
 GigabitEthernet0/8: Other, IP
 GigabitEthernet0/9: Other, IP
 GigabitEthernet0/10: Other, IP
 GigabitEthernet0/11: Other, IP, Spanning Tree, CDP
 GigabitEthernet0/12: Other, IP
 GigabitEthernet0/13: Other, IP, CDP
 GigabitEthernet0/14: Other, IP, Spanning Tree, CDP
 GigabitEthernet0/15: Other, IP, Spanning Tree, CDP
 GigabitEthernet0/16: Other, IP, Spanning Tree, CDP
 GigabitEthernet0/17: Other, IP
 GigabitEthernet0/18: Other, IP
 GigabitEthernet0/19: Other, IP
 GigabitEthernet0/20: Other, IP

<output truncated>
```

This is an example of output from the **show interfaces counters trunk** command. It displays trunk counters for all interfaces.

```
Switch# show interfaces counters trunk
Port        TrunkFramesTx   TrunkFramesRx   WrongEncap
Gi0/1               4207           29123            0
Gi0/2               4207           14672            0
Gi0/3               4230           36486            0
Gi0/4                  0               0            0
Gi0/5                  0               0            0
Gi0/7                  0               0            0
Gi0/8                  0               0            0
Gi0/9                  0               0            0
Gi0/10                 0               0            0
Gi0/11                 0               0            0
Gi0/12                 0               0            0
Gi0/13              4228               0            0
Gi0/14                 0               0            0
Gi0/15                 0               0            0
Gi0/16                 0               0            0
Gi0/17                 0               0            0
Gi0/18                 0               0            0
Gi0/19                 0               0            0
Gi0/20                 0               0            0
Gi0/21                 0               0            0

<output truncated>
```

Related Commands

Command	Description
show interfaces	Displays additional interface characteristics.

show interfaces rep

To display Resilient Ethernet Protocol (REP) configuration and status for a specified interface or for all interfaces, use the **show interfaces rep** command in user EXEC mode.

show interfaces [*interface-id*] **rep** [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) Displays REP configuration and status for a specified physical interface or port channel ID.
detail	(Optional) Displays detailed REP configuration and status information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

In the output for the **show interface rep** [**detail**] command, in addition to an *Open*, *Fail*, or AP (alternate port) state, the Port Role might show as *Fail Logical Open* (*FailLogOpen*) or *Fail No Ext Neighbor* (*FailNoNbr*). These states indicate that the port is physically up, but REP is not configured on the neighboring port. In this case, one port goes into a forwarding state for the data path to help maintain connectivity during configuration. The Port Role for this port shows as Fail Logical Open; the port forwards all data traffic on all VLANs. The other failed Port Role shows as *Fail No Ext Neighbor;* this port blocks traffic for all VLANs.

When the external neighbors for the failed ports are configured, the failed ports go through the alternate port state transitions and eventually go to an Open state or remain as the alternate port, based on the alternate port election mechanism.

In the **show interfaces rep** command output, ports configured as edge no-neighbors are designated with an asterisk (*) in front of *Primary Edge* or *Secondary Edge*. In the output of the **show interfaces rep detail** command, *No-Neighbor* is spelled out.

The output of this command is also included in the **show tech-support** privileged EXEC command output.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is sample output from the **show interface rep** command:

```
Switch # show interface rep
Interface                Seg-id   Type        LinkOp     Role
---------------------- ------ ------------ ----------- ----
GigabitEthernet 0/1        1    Primary Edge  TWO_WAY    Open
GigabitEthernet 0/2        1    Edge          TWO_WAY    Open
FastEthernet 0/4           2                  INIT_DOWN  Fail
```

This is sample output from the **show interface rep** command when the edge port is configured to have no REP neighbor. Note the asterisk (*) next to *Primary Edge*.

```
Switch# show interface rep
Interface              Seg-id Type             LinkOp      Role
---------------------- ------ --------------  ----------- ----
GigabitEthernet0/1     2                      TWO_WAY     Open
GigabitEthernet0/2     2      Primary Edge*   TWO_WAY     Open
```

This is sample output from the **show interface rep** command when external neighbors are not configured:

```
Switch # show interface rep
Interface                Seg-id   Type        LinkOp     Role
---------------------- ------ ------------ ----------- ----
GigabitEthernet0/1         1                NO_NEIGHBOR FailNoNbr
GigabitEthernet0/2         2                NO_NEIGHBOR FailLogOpen
```

This is sample output from the **show interface rep detail** command for a specified interface:

```
Switch # show interface gigabitethernet0/2 rep detail
GigabitEthernet0/2   REP enabled
Segment-id: 1 (Segment)
PortID: 00030019E85BDD00
Preferred flag: No
Operational Link Status: INIT_DOWN
Current Key: 00000000000000000000
Port Role: Fail
Blocked VLAN: 1-4094
Admin-vlan: 1
Preempt Delay Timer: disabled
LSL Ageout Timer: 5000 ms
Configured Load-balancing Block Port: 1234567890123456
Configured Load-balancing Block VLAN: 1-4094
STCN Propagate to: none
LSL PDU rx: 0, tx: 0
HFL PDU rx: 0, tx: 0
BPA TLV rx: 0, tx: 0
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 0, tx: 0
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 0, tx: 0
```

Related Commands

Command	Description
rep segment	Enables REP on an interface and assigns a segment ID. This command is also used to configure a port as an edge port, a primary edge port, or a preferred port.
show rep topology [**detail**]	Displays information about all ports in the segment, including which one was configured and selected as the primary edge port.

show interfaces transceiver

To display the physical properties of a small form-factor pluggable (SFP) module interface, use the **show interfaces transceiver** command in privileged EXEC mode.

show interfaces [*interface-id*] **transceiver** [**detail** | **module** *number* | **properties** | **supported-list** | **threshold-table**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) Displays configuration and status for a specified physical interface.
detail	(Optional) Displays calibration properties, including high and low numbers and any alarm information for any Digital Optical Monitoring (DoM)-capable transceiver if one is installed in the switch.
supported-list	(Optional) Lists all supported DoM transceivers.
threshold-table	(Optional) Displays alarm and warning threshold table. **Note** This keyword displays the thresholds that are programmed into SFP hardware and are not those used to determine when to send alarms or traps. To view those thresholds, enter the **show interfaces transceiver detail** command.
module *number*	(Optional) Limits display to interfaces on module on the switch. The range is 1 to 9. This option is not available if you entered a specific interface ID.
properties	(Optional) Displays speed, duplex, and inline power settings on an interface.
threshold-table	(Optional) Displays alarm and warning threshold table
| begin	(Optional) Display begins with the line that matches the *expression*
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The threshold values shown in the outputs from the **show interfaces transceiver threshold-table** and the **show interfaces transceiver detail** are not the same. The thresholds shown in the output from the **show interfaces transceiver threshold-table** command are hard-coded in Cisco IOS, but are not supported.

The thresholds shown in the output from the **show interfaces transceiver detail** command are read from the SFP EEPROM and are supported. You should always use the **show interfaces transceiver detail** command to view transceiver thresholds.

Examples

This is an example of output from the **show interfaces** *interface-id* **transceiver properties** command:

```
Switch# show interfaces gigabitethernet0/1 transceiver properties
Diagnostic Monitoring is not implemented.
Name : Gi0/1
Administrative Speed: auto
Administrative Duplex: auto
Administrative Auto-MDIX: on
Administrative Power Inline: N/A
Operational Speed: 1000
Operational Duplex: full
Operational Auto-MDIX: on
Media Type: 10/100/1000BaseTX SFP
```

This is an example of output from the **show interfaces transceiver dom-supported-list** command:

```
Switch# show interfaces transceiver dom-supported-list
Transceiver Type           Cisco p/n min version
                               supporting DOM
------------------       -------------------------
   DWDM GBIC                ALL
   DWDM SFP                 ALL
   RX only WDM GBIC         ALL
   DWDM XENPAK              ALL
   DWDM X2                  ALL
   DWDM XFP                 ALL
   CWDM GBIC                NONE
   CWDM X2                  ALL
   CWDM XFP                 ALL
   XENPAK ZR                ALL
   X2 ZR                    ALL
   XFP ZR                   ALL
   Rx_only_WDM_XENPAK       ALL
   XENPAK_ER                10-1888-03
   X2_ER                    ALL
   XFP_ER                   ALL
   XENPAK_LR                10-1838-04
   X2_LR                    ALL
   <output truncated>
```

This is an example of output from the **show interfaces transceiver threshold-table** command. Note that these are thresholds programmed into IOS software, and are NOT used to determine alarms.

```
Optical Tx     Optical Rx    Temp     Laser Bias    Voltage
                                                    current
             -------------  -------------  ------   ------------  ---------

 DWDM GBIC
Min1             -0.50        -28.50        0            N/A          4.50
Min2             -0.30        -28.29        5            N/A          4.75
Max2              3.29         -6.69        60           N/A          5.25
Max1              3.50          6.00        70           N/A          5.50
 DWDM SFP
Min1             -0.50        -28.50        0            N/A          3.00
Min2             -0.30        -28.29        5            N/A          3.09
Max2              4.30         -9.50        60           N/A          3.59
Max1              4.50          9.30        70           N/A          3.70
 RX only WDM GBIC
Min1              N/A         -28.50        0            N/A          4.50
Min2              N/A         -28.29        5            N/A          4.75
Max2              N/A          -6.69        60           N/A          5.25
Max1              N/A           6.00        70           N/A          5.50
 DWDM XENPAK
Min1             -1.50        -24.50        0            N/A          N/A
```

```
Min2              -1.29        -24.29        5             N/A           N/A
Max2               3.29         -6.69        60            N/A           N/A
Max1               3.50          4.00        70            N/A           N/A
 DWDM X2
Min1              -1.50        -24.50        0             N/A           N/A
Min2              -1.29        -24.29        5             N/A           N/A
Max2               3.29         -6.69        60            N/A           N/A
Max1               3.50          4.00        70            N/A           N/A
 DWDM XFP
Min1              -1.50        -24.50        0             N/A           N/A
Min2              -1.29        -24.29        5             N/A           N/A
Max2               3.29         -6.69        60            N/A           N/A
Max1               3.50          4.00        70            N/A           N/A
 CWDM X2
Min1               N/A           N/A         0             N/A           N/A
Min2               N/A           N/A         0             N/A           N/A
Max2               N/A           N/A         0             N/A           N/A
Max1               N/A           N/A         0             N/A           N/A
```

Related Commands

Command	Description
show interfaces	Displays additional interface characteristics.

show inventory

To display product identification (PID) information for the hardware, use the **show inventory** command in user EXEC mode.

show inventory [*entity-name* | **raw**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

entity-name	(Optional) Displays the specified entity. For example, enter the interface (such as gigabitethernet 0/x) into which a small form-factor pluggable (SFP) module is installed to display its identity.
raw	(Optional) Displays every entity in the device.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The command is case sensitive. With no arguments, the **show inventory** command produces a compact display of all identifiable entities that have a product identifier. The display shows the entity location (slot identity), entity description, and the unique device identifier (UDI), including PID, version identifier (VID), and serial number (SN) of that entity.

Many legacy SFPs are not programmed with PIDs and VID.s

Note If there is no PID, no output appears when you enter the **show inventory** command.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is example output from the **show inventory** command:

```
Switch> show inventory
NAME: "1", DESCR: "model-id"
PID: model-id , VID:Vo1 , SN: FSJC0407839

NAME: "GigabitEthernet0/1", DESCR: "100BaseBX-10U SFP"
PID:                     , VID:    , SN: NEC08440067
NAME: "GigabitEthernet0/2", DESCR: "10/100/1000BaseTX SFP"
PID:                     , VID:    , SN: 00000MTC0839048G
```

show ip igmp profile

To display all configured Internet Group Management Protocol (IGMP) profiles or a specified IGMP profile, use the **show ip igmp profile** command in privileged EXEC mode.

show ip igmp profile [*profile number*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

profile number	(Optional) The IGMP profile number to be displayed. The range is 1 to 4294967295. If no profile number is entered, all IGMP profiles are displayed.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History52

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

These are examples of output from the **show ip igmp profile** privileged EXEC command, with and without specifying a profile number. If no profile number is entered, the display includes all profiles configured on the switch.

```
Switch# show ip igmp profile 40
IGMP Profile 40
    permit
    range 233.1.1.1 233.255.255.255

Switch# show ip igmp profile
IGMP Profile 3
    range 230.9.9.0 230.9.9.0
IGMP Profile 4
    permit
    range 229.9.9.0 229.255.255.255
```

Related Commands

Command	Description
ip igmp profile	Configures the specified IGMP profile number.

show ip igmp snooping

To display the Internet Group Management Protocol (IGMP) snooping configuration of the switch or the VLAN, use the **show ip igmp snooping** command in user EXEC mode.

show ip igmp snooping [**groups** | **mrouter** | **querier** [**vlan** *vlan-id*] **[detail]**] [**vlan** *vlan-id*] **[detail]** [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

groups	(Optional) See the **show ip igmp snooping groups** command.
mrouter	(Optional) See the **show ip igmp snooping mrouter** command.
querier	(Optional) See the **show ip igmp snooping querier** command.
vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094 (available only in privileged EXEC mode).
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Although visible in the command line interface help, the **querier** keyword is not supported.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use this command to display snooping configuration for the switch or for a specific VLAN.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Although visible in the output display, output lines for source-only learning are not valid.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show ip igmp snooping vlan 1** command. It shows snooping characteristics for a specific VLAN.

```
Switch# show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping             :Enabled
IGMPv3 snooping (minimal) :Enabled
Report suppression        :Enabled
```

```
TCN solicit query         :Disabled
TCN flood query count     :2
Last member query interval : 100


Vlan 1:
--------
IGMP snooping                        :Enabled
Immediate leave                      :Disabled
Multicast router learning mode       :pim-dvmrp
Source only learning age timer       :10
CGMP interoperability mode           :IGMP_ONLY
Last member query interval : 100
```

Note Source-only learning are not supported, and information appearing for this feature is not valid.

This is an example of output from the **show ip igmp snooping** command. It displays snooping characteristics for all VLANs on the switch.

```
Switch> show ip igmp snooping
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping               : Enabled
IGMPv3 snooping (minimal)   : Enabled
Report suppression          : Enabled
TCN solicit query           : Disabled
TCN flood query count       : 2
Last member query interval : 100

Vlan 1:
--------
IGMP snooping                        :Enabled
Immediate leave                      :Disabled
Multicast router learning mode       :pim-dvmrp
Source only learning age timer       :10
CGMP interoperability mode           :IGMP_ONLY
Last member query interval           : 100

Vlan 2:
--------
IGMP snooping                        :Enabled
Immediate leave                      :Disabled
Multicast router learning mode       :pim-dvmrp
Source only learning age timer       :10
CGMP interoperability mode           :IGMP_ONLY
Last member query interval           : 333

<output truncated>
```

Related Commands

Command	Description
ip igmp snooping	Enables and configures IGMP snooping on the switch or on a VLAN.
show ip igmp snooping mrouter	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.
show ip igmp snooping querier	Displays the configuration and operation information for the IGMP querier configured on a switch.

show ip igmp snooping groups

To display the Internet Group Management Protocol (IGMP) snooping multicast table or multicast information for the switch, use the **show ip igmp snooping groups** command in privileged EXEC command. To display the multicast table for a specified multicast VLAN or to diplay specific multicast information, use with the **vlan** keyword.

show ip igmp snooping groups [**count**] [**|** {**begin | exclude | include**} *expression*]

show ip igmp snooping groups vlan *vlan-id* [*ip_address* **|** **count**] [**|** {**begin | exclude | include**} *expression*]

Syntax Description

count	(Optional) Displays the total number of entries for the specified command options instead of the actual entries.
ip_address	(Optional) Displays characteristics of the multicast group with the specified group IP address.
vlan-id	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use this command to display multicast information or the multicast table.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show ip igmp snooping groups** command without any keywords. It displays the multicast table for the switch.

```
Switch# show ip igmp snooping groups
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi0/1, Gi0/2
104       224.1.4.3       igmp        v2          Gi0/1, Gi0/2
```

This is an example of output from the **show ip igmp snooping groups count** command. It displays the total number of multicast groups on the switch.

```
Switch# show ip igmp snooping groups count
Total number of multicast groups: 2
```

This is an example of output from the **show ip igmp snooping groups vlan** *vlan-id ip-address* command. It shows the entries for the group with the specified IP address.

```
Switch# show ip igmp snooping groups vlan 104 224.1.4.2
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi0/1, Gi0/5
```

Related Commands

Command	Description
ip igmp snooping	Enables and configures IGMP snooping on the switch or on a VLAN.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or the VLAN.
show ip igmp snooping mrouter	Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN.

show ip igmp snooping mrouter

To display the Internet Group Management Protocol (IGMP) snooping dynamically learned and manually configured multicast router ports for the switch or for the specified multicast VLAN, use the **show ip igmp snooping mrouter** command in privileged EXEC mode.

show ip igmp snooping mrouter [**vlan** *vlan-id*] [**|** {**begin | exclude | include**} *expression*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use this command to display multicast router ports on the switch or for a specific VLAN.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show ip igmp snooping mrouter** command. It shows how to display multicast router ports on the switch.

```
Switch# show ip igmp snooping mrouter
Vlan    ports
----    -----
   1    Gi0/1(dynamic)
```

Related Commands

Command	Description
ip igmp snooping	Enables and configures IGMP snooping on the switch or a VLAN.
ip igmp snooping vlan mrouter	Adds a multicast router port to a multicast VLAN.
show ip igmp snooping	Displays the IGMP snooping configuration of the switch or VLAN.
show ip igmp snooping groups	Displays IGMP snooping multicast information for the switch or for the specified parameter.

show ipc

To display Interprocess Communications Protocol (IPC) configuration, status, and statistics, use the **show ipc** command in user EXEC mode.

show ipc {**hog-info** | **mcast** {**appclass** | **groups** | **status**} | **nodes** | **ports** [**open**] | **queue** | **rpc** | **session** {**all** | **rx** | **tx**} [**verbose**] | **status** [**cumlulative**] | **zones**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

mcast {**appclass** | **groups** | **status**}	Displays the IPC multicast routing information. The keywords have these meanings: • **appclass**—Display the IPC multicast application classes. • **groups**—Display the IPC multicast groups. • **status**—Display the IPC multicast routing status.
nodes	Displays participating nodes.
ports [**open**]	Displays local IPC ports. The keyword has this meaning: • **open**—(Optional) Display only the open ports.
queue	Displays the contents of the IPC transmission queue.
rpc	Displays the IPC remote-procedure statistics.
session {**all** | **rx** | **tx**}	Displays the IPC session statistics (available only in privileged EXEC mode). The keywords have these meanings: • **all**—Display all the session statistics. • **rx**—Display the sessions statistics for traffic that the switch receives • **tx**—Display the sessions statistics for traffic that the switch forwards.
verbose	(Optional) Displays detailed statistics (available only in privileged EXEC mode).
status [**cumlulative**]	Displays the status of the local IPC server. The keyword has this meaning: • **cumlulative**—(Optional) Display the status of the local IPC server since the switch was started or restarted.
zones	Displays participating IPC zones. The switch supports one IPC zone.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This example shows how to display the IPC routing status:

```
Switch> show ipc mcast status
                          IPC Mcast Status
                                                              Tx        Rx

 Total Frames                                                 0         0
 Total control Frames                                         0         0
 Total Frames dropped                                         0         0
 Total control Frames dropped                                 0         0

 Total Reliable messages                                      0         0
 Total Reliable messages acknowledged                         0         0
 Total Out of Band Messages                                   0         0
 Total Out of Band messages acknowledged                      0         0

 Total No Mcast groups                                        0         0

 Total Retries                    0  Total Timeouts                    0
 Total OOB Retries                0  Total OOB Timeouts                0
 Total flushes                    0  Total No ports                    0
```

This example shows how to display the participating nodes:

```
Switch> show ipc nodes
There is 1 node in this IPC realm.
   ID    Type       Name           Last  Last
                                   Sent  Heard
   10000 Local      IPC Master     0      0
```

This example shows how to display the local IPC ports:

```
Switch> show ipc ports
There are 8 ports defined.

Port ID        Type       Name                    (current/peak/total)
There are 8 ports defined.
   10000.1     unicast    IPC Master:Zone
   10000.2     unicast    IPC Master:Echo
   10000.3     unicast    IPC Master:Control
   10000.4     unicast    IPC Master:Init
   10000.5     unicast    FIB Master:DFS.process_level.msgs
   10000.6     unicast    FIB Master:DFS.interrupt.msgs
   10000.7     unicast    MDFS RP:Statistics
     port_index = 0  seat_id = 0x10000    last sent = 0     last heard = 0
  0/2/159

   10000.8     unicast    Slot 1 :MDFS.control.RIL
     port_index = 0  seat_id = 0x10000    last sent = 0     last heard = 0
  0/0/0

RPC packets:current/peak/total
                                                              0/1/4
```

This example shows how to display the contents of the IPC retransmission queue:

```
Switch> show ipc queue
There are 0 IPC messages waiting for acknowledgement in the transmit queue.
There are 0 IPC messages waiting for a response.
There are 0 IPC messages waiting for additional fragments.
There are 0 IPC messages currently on the IPC inboundQ.
Messages currently in use                    :         3
Message cache size                           :      1000
Maximum message cache usage                  :      1000

0  times message cache crossed       5000 [max]

Emergency messages currently in use          :         0

There are 2 messages currently reserved for reply msg.

Inbound message queue depth 0
Zone inbound message queue depth 0
```

This example shows how to display all the IPC session statistics:

```
Switch# show ipc session all
Tx Sessions:
Port ID        Type       Name
   10000.7     Unicast    MDFS RP:Statistics
     port_index = 0  type = Unreliable      last sent = 0     last heard = 0
     Msgs requested = 180  Msgs returned = 180

   10000.8     Unicast    Slot 1 :MDFS.control.RIL
     port_index = 0  type = Reliable        last sent = 0     last heard = 0
     Msgs requested = 0    Msgs returned = 0

Rx Sessions:
Port ID        Type       Name
   10000.7     Unicast    MDFS RP:Statistics
     port_index = 0  seat_id = 0x10000    last sent = 0     last heard = 0
     No of msgs requested = 180   Msgs returned = 180

   10000.8     Unicast    Slot 1 :MDFS.control.RIL
     port_index = 0  seat_id = 0x10000    last sent = 0     last heard = 0
     No of msgs requested = 0     Msgs returned = 0
```

This example shows how to display the status of the local IPC server:

```
Switch> show ipc status cumulative
                        IPC System Status

 Time last IPC stat cleared :never

 This processor is the IPC master server.
 Do not drop output of IPC frames for test purposes.

 1000 IPC Message Headers Cached.

                                                    Rx Side     Tx Side

 Total Frames                                         12916         608
     0          0
 Total from Local Ports                               13080         574
 Total Protocol Control Frames                          116          17
 Total Frames Dropped                                     0           0

                             Service Usage
```

```
 Total via Unreliable Connection-Less Service            12783         171
 Total via Unreliable Sequenced Connection-Less Svc          0           0
 Total via Reliable Connection-Oriented Service             17         116

<output truncated>
```

Related Commands

Command	Description
clear ipc	Clears the IPC multicast routing statistics.

show lacp

To display Link Aggregation Control Protocol (LACP) channel-group information, use the **show lacp** command in user EXEC mode.

show lacp [*channel-group-number*] {**counters** | **internal** | **neighbor** | **sys-id**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

channel-group-number	(Optional) Number of the channel group. The range is 1 to 26.
counters	Displays traffic information.
internal	Displays internal information.
neighbor	Displays neighbor information.
sys-id	Displays the system identifier that is being used by LACP. The system identifier is made up of the LACP system priority and the switch MAC address.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can enter any **show lacp** command to display the active channel-group information. To display specific channel information, enter the **show lacp** command with a channel-group number.

If you do not specify a channel group, information for all channel groups appears.

You can enter the *channel-group-number* option to specify a channel group for all keywords except **sys-id**.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show lacp counters** user EXEC command. Table 2-16 describes the fields in the display.

```
Switch> show lacp counters
               LACPDUs          Marker      Marker Response    LACPDUs
Port         Sent   Recv      Sent   Recv      Sent   Recv      Pkts Err
--------------------------------------------------------------------
Channel group:1
Gi0/1        19     10        0      0         0      0         0
Gi0/2        14     6         0      0         0      0         0
```

Table 3-12 show lacp counters Field Descriptions

Field	Description
LACPDUs Sent and Recv	The number of LACP packets sent and received by a port.
Marker Sent and Recv	The number of LACP marker packets sent and received by a port.
Marker Response Sent and Recv	The number of LACP marker response packets sent and received by a port.
LACPDUs Pkts and Err	The number of unknown and illegal packets received by LACP for a port.

This is an example of output from the **show lacp internal** command:

```
Switch> show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port     Port
Port        Flags   State   Priority      Key       Key     Number   State
Gi0/1       SA      bndl    32768         0x3       0x3     0x4      0x3D
Gi0/2       SA      bndl    32768         0x3       0x3     0x5      0x3D
```

Table 2-17 describes the fields in the display.

Table 3-13 show lacp internal Field Descriptions

Field	Description
State	State of the specific port. These are the allowed values: • – —Port is in an unknown state. • **bndl**—Port is attached to an aggregator and bundled with other ports. • **susp**—Port is in a suspended state; it is not attached to any aggregator. • **hot-sby**—Port is in a hot-standby state. • **indiv**—Port is incapable of bundling with any other port. • **indep**—Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port). • **down**—Port is down.
LACP Port Priority	Port priority setting. LACP uses the port priority to put ports s in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
Admin Key	Administrative key assigned to this port. LACP automatically generates an administrative key value as a hexadecimal number. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by the port physical characteristics (for example, data rate and duplex capability) and configuration restrictions that you establish.
Oper Key	Runtime operational key that is being used by this port. LACP automatically generates this value as a hexadecimal number.

Table 3-13 show lacp internal Field Descriptions (continued)

Field	Description
Port Number	Port number.
Port State	State variables for the port, encoded as individual bits within a single octet with these meanings: • bit0: LACP_Activity • bit1: LACP_Timeout • bit2: Aggregation • bit3: Synchronization • bit4: Collecting • bit5: Distributing • bit6: Defaulted • bit7: Expired **Note** In the above list, bit7 is the MSB and bit0 is the LSB.

This is an example of output from the **show lacp neighbor** command:

```
Switch> show lacp neighbor
Flags:  S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 3 neighbors

Partner's information:

          Partner               Partner                     Partner
Port      System ID             Port Number     Age         Flags
Gi0/1     32768,0007.eb49.5e80  0xC               19s       SP

          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          32768                 0x3             0x3C

Partner's information:

          Partner               Partner                     Partner
Port      System ID             Port Number     Age         Flags
Gi0/2     32768,0007.eb49.5e80  0xD               15s       SP

          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          32768                 0x3             0x3C
```

This is an example of output from the **show lacp sys-id** command:

```
Switch> show lacp sys-id
32765,0002.4b29.3a00
```

The system identification is made up of the system priority and the system MAC address. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC address associated to the system.

Related Commands

Command	Description
clear lacp	Clears the LACP channel-group information.
lacp port-priority	Configures the LACP port priority.
lacp system-priority	Configures the LACP system priority.

show location

To display location information for a Link Layer Discovery Protocol (LLDP) endpoint, use the **show location** command in user EXEC mode.

show location admin-tag | [| {**begin** | **exclude** | **include**} *expression*]

show location civic-location {**identifier** *id number* | **interface** *interface-id* | **static**} | [| {**begin** | **exclude** | **include**} *expression*]

show location elin-location {**identifier** *id number* | **interface** *interface-id* | **static**} | [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

admin-tag	Displays administrative tag or site information.
civic-location	Displays civic location information.
elin-location	Displays emergency location information (ELIN).
identifier *id*	Specifies the ID for the civic location or the elin location. The id range is 1 to 4095.
interface *interface-id*	Displays location information for the specified interface or all interfaces. Valid interfaces include physical ports.
static	Displays static configuration information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use the **show location** command to display location information for an endpoint.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show location civic-location** command that displays location information for an interface:

```
Switch> show location civic interface gigabitethernet 0/1
Civic location information
--------------------------
Identifier              : 1
County                  : Santa Clara
Street number           : 3550
Building                : 19
Room                    : C6
Primary road name       : Cisco Way
City                    : San Jose
State                   : CA
Country                 : US
```

This is an example of output from the **show location civic-location** command that displays all the civic location information:

```
Switch> show location civic-location static
Civic location information
--------------------------
Identifier              : 1
County                  : Santa Clara
Street number           : 3550
Building                : 19
Room                    : C6
Primary road name       : Cisco Way
City                    : San Jose
State                   : CA
Country                 : US
Ports                   : Gi0/1
--------------------------
Identifier              : 2
Street number           : 24568
Street number suffix    : West
Landmark                : Golden Gate Bridge
Primary road name       : 19th Ave
City                    : San Francisco
Country                 : US
--------------------------
```

This is an example of output from the **show location elin-location** command that displays the emergency location information:

```
Switch> show location elin-location identifier 1
Elin location information
--------------------------
Identifier : 1
Elin       : 14085553881
Ports      : Gi0/2
```

This is an example of output from the **show location elin static** command that displays all emergency location information:

```
Switch> show location elin static
Elin location information
--------------------------
Identifier : 1
Elin       : 14085553881
Ports      : Gi0/2
--------------------------
Identifier : 2
Elin       : 18002228999
--------------------------
```

Related Commands

Command	Description
location (global configuration)	Configures the global location information for an endpoint.
location (interface configuration)	Configures the location information for an interface.

show logging onboard

To display the on-board failure logging (OBFL) information, use the **show logging onboard** command in privileged EXEC mode.

show logging onboard [**module** [*slot-number*]] [**clilog | environment | message |temperature | uptime | voltage**] [**continuous | detail | summary**] [**start** *hh:mm:ss day month year*] [**end** *hh:mm:ss day month year*]} [| {**begin | exclude | include**} *expression*]

Syntax Description

module [*slot-number*]	(Optional) The **module** slot number is always 1 and is not relevant for the switch.
clilog	Displays the OBFL CLI commands that were entered on the switch.
environment	Displays the unique device identifier (UDI) information for the switch and for all the connected devices: the product identification (PID), the version identification (VID), and the serial number.
message	Displays the hardware-related system messages generated by the switch.
temperature	Displays the temperature of the switch.
uptime	Displays the time when the switch starts, the reason the switch restarts, and the length of time the switch has been running since it last restarted.
voltage	Displays the system voltages of the switch.
continuous	(Optional) Displays the data in the *continuous* file. For more information, see the "Usage Guidelines" section.
summary	(Optional) Displays the data in the *summary* file. For more information, see the "Usage Guidelines" section.
start *hh:mm:ss day month year*	(Optional) Displays the data from the specified time and date. For more information, see the "Usage Guidelines" section.
end *hh:mm:ss day month year*	(Optional) Displays the data up to the specified time and date. For more information, see the "Usage Guidelines" section.
detail	(Optional) Displays both the continuous and summary data.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When OBFL is enabled, the switch records all the OBFL data in a continuous, circular file. When the continuous file is full, the switch combines the data into a summary file, which is also known as a historical file. The switch then continues to write new data to the continuous file.

Use the **start** and **end** keywords to display data collected only during a particular time period. When specifying the **start** and **end** times, follow these guidelines:

- *hh:mm:ss*—Enter the time as a 2-digit number for a 24-hour clock. Make sure to use the colons (:). For example, enter **13:32:45**.
- *day*—Enter the day of the month. The range is from 1 to 31.
- *month*—Enter the month in upper-case or lower-case letters. You can enter the full name of the month, such as **January** or **august**, or the first three letters of the month, such as **jan** or **Aug**.
- *year*—Enter the year as a 4-digit number, such as 2008. The range is from 1993 to 2035.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show logging onboard clilog continuous** command:

```
Switch# show logging onboard clilog continuous
--------------------------------------------------------------------------------
CLI LOGGING CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
MM/DD/YYYY HH:MM:SS COMMAND
--------------------------------------------------------------------------------
05/12/2006 15:33:17 show logging onboard temperature detail
05/12/2006 15:33:21 show logging onboard voltage detail
05/12/2006 16:14:09 show logging onboard temperature summary
...
<output truncated>
....
05/16/2006 13:07:53 no hw-module module logging onboard message level
05/16/2006 13:16:13 show logging onboard uptime continuous
05/16/2006 13:39:18 show logging onboard uptime summary
05/16/2006 13:45:57 show logging onboard clilog summary
--------------------------------------------------------------------------------
```

This is an example of output from the **show logging onboard message** command:

```
Switch# show logging onboard message
--------------------------------------------------------------------------------
ERROR MESSAGE SUMMARY INFORMATION
--------------------------------------------------------------------------------
Facility-Sev-Name      | Count | Persistence Flag
MM/DD/YYYY HH:MM:SS
--------------------------------------------------------------------------------
No historical data to display
--------------------------------------------------------------------------------
```

This is an example of output from the **show logging onboard status** command:

```
Switch# show logging onboard status
Devices registered with infra
                Slot no.: 0 Subslot no.: 0, Device obfl0:
Application name clilog :
                Path : obfl0:
                CLI enable status  : enabled
                Platform enable status: enabled
Application name environment :
                Path : obfl0:
                CLI enable status  : enabled
                Platform enable status: enabled
Application name errmsg :
                Path : obfl0:
                CLI enable status  : enabled
                Platform enable status: enabled
Application name poe :
                Path : obfl0:
                CLI enable status  : enabled
                Platform enable status: enabled
Application name temperature :
                Path : obfl0:
                CLI enable status  : enabled
                Platform enable status: enabled
Application name uptime :
                Path : obfl0:
                CLI enable status  : enabled
                Platform enable status: enabled
Application name voltage :
                Path : obfl0:
                CLI enable status  : enabled
                Platform enable status: enabled
```

This is an example of output from the **show logging onboard temperature continuous** command:

```
Switch# show logging onboard temperature continuous
-------------------------------------------------------------------------------
TEMPERATURE CONTINUOUS INFORMATION
-------------------------------------------------------------------------------
Sensor                            |   ID  |
-------------------------------------------------------------------------------
Board temperature                          1

-------------------------------------------------------------------------------
       Time Stamp    |Sensor Temperature 0C
MM/DD/YYYY HH:MM:SS |  1    2    3    4    5    6    7    8    9   10   11   12
-------------------------------------------------------------------------------
05/12/2006 15:33:20   35   --   --   --   --   --   --   --   --   --   --   --
05/12/2006 16:31:21   35   --   --   --   --   --   --   --   --   --   --   --
05/12/2006 17:31:21   35   --   --   --   --   --   --   --   --   --   --   --
05/12/2006 18:31:21   35   --   --   --   --   --   --   --   --   --   --   --
05/12/2006 19:31:21   35   --   --   --   --   --   --   --   --   --   --   --
05/12/2006 20:31:21   35   --   --   --   --   --   --   --   --   --   --   --
05/12/2006 21:29:22   35   --   --   --   --   --   --   --   --   --   --   --
05/12/2006 22:29:22   35   --   --   --   --   --   --   --   --   --   --   --
05/12/2006 23:29:22   35   --   --   --   --   --   --   --   --   --   --   --
05/13/2006 00:29:22   35   --   --   --   --   --   --   --   --   --   --   --
05/13/2006 01:29:22   35   --   --   --   --   --   --   --   --   --   --   --
05/13/2006 02:27:23   35   --   --   --   --   --   --   --   --   --   --   --
05/13/2006 03:27:23   35   --   --   --   --   --   --   --   --   --   --   --
05/13/2006 04:27:23   35   --   --   --   --   --   --   --   --   --   --   --
05/13/2006 05:27:23   35   --   --   --   --   --   --   --   --   --   --   --
05/13/2006 06:27:23   35   --   --   --   --   --   --   --   --   --   --   --
```

```
05/13/2006 07:25:24   36   --   --   --   --   --   --   --   --   --   --   --
05/13/2006 08:25:24   35   --   --   --   --   --   --   --   --   --   --   --
<output truncated>
```

This is an example of output from the **show logging onboard uptime summary** command:

```
Switch# show logging onboard uptime summary
-------------------------------------------------------------------------------
UPTIME SUMMARY INFORMATION
-------------------------------------------------------------------------------
First customer power on : 03/01/1993 00:03:50
Total uptime            :   0 years   0 weeks   3 days  21 hours  55 minutes
Total downtime          :   0 years   0 weeks   0 days   0 hours   0 minutes
Number of resets        : 2
Number of slot changes  : 1
Current reset reason    : 0x0
Current reset timestamp : 03/01/1993 00:03:28
Current slot            : 1
Current uptime          :   0 years   0 weeks   0 days   0 hours  55 minutes
-------------------------------------------------------------------------------
Reset  |        |
Reason | Count  |
-------------------------------------------------------------------------------
No historical data to display
-------------------------------------------------------------------------------
```

This is an example of output from the **show logging onboard voltage summary** command:

```
Switch# show logging onboard voltage summary
-------------------------------------------------------------------------------
VOLTAGE SUMMARY INFORMATION
-------------------------------------------------------------------------------
Number of sensors          : 8
Sampling frequency         : 60 seconds
Maximum time of storage    : 3600 minutes
-------------------------------------------------------------------------------
Sensor                            |   ID  | Maximum Voltage
-------------------------------------------------------------------------------
12.00V                              0      12.567
5.00V                               1       5.198
3.30V                               2       3.439
2.50V                               3       2.594
1.50V                               4       1.556
1.20V                               5       1.239
1.00V                               6       0.980
0.75V                               7       0.768
-------------------------------------------------------------------------------
Nominal Range                         Sensor ID

-------------------------------------------------------------------------------
No historical data to display
-------------------------------------------------------------------------------
```

Related Commands

Command	Description
clear logging onboard	Removes the OBFL data in the flash memory.
hw-module module logging onboard	Enables OBFL.

show mac access-group

To display the MAC access control lists (ACLs) configured for an interface or a switch, use the **show mac access-group** command in user EXEC mode.

show mac access-group [**interface** *interface-id*] [**|** {**begin | exclude | include**} *expression*]

Syntax Description

interface *interface-id*	(Optional) Displays the MAC ACLs configured on a specific interface. Valid interfaces are physical ports and port channels; the port-channel range is 1 to 48 (available only in privileged EXEC mode).
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac-access group** user EXEC command. In this display, Gigabit Ethernet interface 0/2 has the MAC access list *macl_e1* applied to inbound traffic; no MAC ACLs are applied to other interfaces.

```
Switch> show mac access-group
Interface GigabitEthernet0/1:
   Inbound access-list is macl_e1
   Outbound access-list is not set
Interface GigabitEthernet0/2:
   Inbound access-list is not set
   Outbound access-list is not set
Interface GigabitEthernet0/3:
   Inbound access-list is not set
   Outbound access-list is not set
Interface GigabitEthernet0/4:
   Inbound access-list is not set
   Outbound access-list is not set
Interface GigabitEthernet0/5:
   Inbound access-list is not set
   Outbound access-list is not set
<output truncated>
```

This is an example of output from the **show mac access-group interface gigabitethernet0/1** command:

```
Switch# show mac access-group interface gigabitethernet0/1
Interface GigabitEthernet0/1:
   Inbound access-list is macl_e1
```

Related Commands

Command	Description
mac access-group	Applies a MAC access group to an interface.

show mac address-table

To display a specific MAC address table static and dynamic entry, or the MAC address table static and dynamic entries on a specific interface or VLAN, use the **show mac address-table** command in user EXEC mode.

show mac address-table [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table** command:

```
Switch> show mac address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type       Ports
----    -----------       ----       -----
 All    0000.0000.0001    STATIC     CPU
 All    0000.0000.0002    STATIC     CPU
 All    0000.0000.0003    STATIC     CPU
 All    0000.0000.0009    STATIC     CPU
 All    0000.0000.0012    STATIC     CPU
 All    0180.c200.000b    STATIC     CPU
 All    0180.c200.000c    STATIC     CPU
 All    0180.c200.000d    STATIC     CPU
 All    0180.c200.000e    STATIC     CPU
 All    0180.c200.000f    STATIC     CPU
 All    0180.c200.0010    STATIC     CPU
   1    0030.9441.6327    DYNAMIC    Gi0/4
Total Mac Addresses for this criterion: 12
```

Related Commands

Command	Description
clear mac address-table dynamic	Deletes from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table address

To display MAC address table information for the specified MAC address, use the **show mac address-table address** command in user EXEC mode.

show mac address-table address *mac-address* [**bridge-domain** *number*] [**interface** *interface-id*] [**vlan** *vlan-id*] [**|** {**begin | exclude | include**} *expression*]

Syntax Description

mac-address	Specifies the 48-bit MAC address; the valid format is H.H.H.
bridge-domain *number*]	(Optional) Displays information for the specified Ethernet Flow Point (EFP) bridge domain. The range is from 1 to 8000.
interface *interface-id*	(Optional) Displays information for a specific interface. Valid interfaces include physical ports and port channels.
vlan *vlan-id*	(Optional) Displays entries for the specific VLAN only. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table address** command:

```
Switch# show mac address-table address 0014.c23b.3573
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0014.c23b.3573    DYNAMIC     Gi0/5
   3    0014.c23b.3573    DYNAMIC     Gi0/2+Efp66
Total Mac Addresses for this criterion: 2
```

Related Commands

Command	Description
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table aging-time

To display the aging time of a specific address table instance, or all address table instances on a specified VLAN or bridge domain or on all VLANs and bridge domains, use the **show mac address-table aging-time** command in user EXEC mode.

show mac address-table aging-time [**bridge-domain** *number*] [**routed-mac**] [**vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

bridge-domain *number*	(Optional) Displays aging time for the specified Ethernet Flow Point (EFP) bridge domain. The range is from 1 to 8000.
routed-mac	(Optional) Displays aging time for routed MAC addresses.
vlan *vlan-id*	(Optional) Displays aging time information for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If no VLAN number is specified, the aging time for all VLANs appears.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table aging-time** command:

```
Switch> show mac address-table aging-time
Global Aging Time:  300
Vlan    Aging Time
----    ----------
```

This is an example of output from the **show mac address-table aging-time vlan 10** command:

```
Switch> show mac address-table aging-time vlan 10
Vlan    Aging Time
----    ----------
  10     300
```

This is an example of output from the **show mac address-table aging-time** for a bridge domain:

```
Switch> show mac address-table aging-time bridge-domain 66
Global Aging Time:  300
BD      Aging Time
----    ----------
 66       200
```

Related Commands

Command	Description
mac address-table aging-time	Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table bridge-domain

To display the MAC address table information for the specified bridge domain, use the **show mac address-table bridge-domain** command in user EXEC mode.

show mac address-table bridge-domain *number* [**|** {**begin | exclude | include**} *expression*]

Syntax Description

number	Specifies the Ethernet Flow Point (EFP) bridge domain number. The range is 1 to 8000.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table bridge-domain** command:

```
Switch> show mac address-table interface bridge-domain 2
          Mac Address Table
------------------------------------------
BD      Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0000.0000    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0ccc.ccce    STATIC      CPU
 All    0100.0ccd.cdd0    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
```

```
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
Total Mac Addresses for this criterion: 24
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table count

To display the number of addresses present in all VLANs or the specified VLAN, use the **show mac address-table count** command in user EXEC mode.

show mac address-table count [**bridge-domain** *number*] [**vlan** *vlan-id*] [**|** {**begin | exclude | include**} *expression*]

Syntax Description

bridge-domain *number*	(Optional) Displays the number of addresses for a specific Ethernet Flow Point (EFP) bridge domain. The range is 1 to 8000.
vlan *vlan-id*	(Optional) Displays the number of addresses for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If no VLAN number is specified, the address count for all VLANs appears.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table count** command:

```
Switch# show mac address-table count
Mac Entries for vlan 1:
---------------------------
Dynamic Address Count  : 69
Static  Address Count  : 0
Total Mac Addresses    : 69

Mac Entries for vlan 2:
---------------------------
Dynamic Address Count  : 0
Static  Address Count  : 0
Total Mac Addresses    : 0

Mac Entries for vlan 3:
---------------------------
Dynamic Address Count  : 52
Static  Address Count  : 0
Total Mac Addresses    : 52
```

```
Mac Entries for vlan 44:
---------------------------
Dynamic Address Count  : 0
Static  Address Count  : 0
Total Mac Addresses    : 0

Total Mac Address Space Available: 255879
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table dynamic

To display only dynamic MAC address table entries, use the **show mac address-table dynamic** command in user EXEC mode.

show mac address-table dynamic [**address** *mac-address*] [**bridge-domain** *number*] [**interface** *interface-id*] [**vlan** *vlan-id*] [**|** {**begin | exclude | include**} *expression*]

Syntax Description

address *mac-address*	(Optional) Specifies a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only).
bridge-domain *number*	(Optional) Displays entries for a specific Ethernet Flow Point (EFP) bridge domain number. The range is from 1 to 8000.
interface *interface-id*	(Optional) Displays entries for a specific interface. Valid *interfaces* are physical ports and port channels.
vlan *vlan-id*	(Optional) Displays entries for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table dynamic** command:

```
Switch> show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0003.e386.47f0    DYNAMIC     Gi0/5
   1    0009.9b00.dd9d    DYNAMIC     Gi0/5
   1    0009.9b01.2d25    DYNAMIC     Gi0/5
   1    000c.2925.7d4d    DYNAMIC     Gi0/5
   1    000c.298f.0d15    DYNAMIC     Gi0/5
   1    000c.299b.b392    DYNAMIC     Gi0/5
   1    000c.29d8.3445    DYNAMIC     Gi0/5
   1    000e.0c9c.3af4    DYNAMIC     Gi0/5
   1    000e.0ca8.44c8    DYNAMIC     Gi0/5
   1    000e.0cab.2012    DYNAMIC     Gi0/5
   1    000e.0cb8.88d1    DYNAMIC     Gi0/5
```

```
   1    0011.1195.1574    DYNAMIC     Gi0/5
   1    0011.1195.157c    DYNAMIC     Gi0/5
   1    0011.11f1.ee7c    DYNAMIC     Gi0/5
   1    0011.929c.5f58    DYNAMIC     Gi0/5
<output truncated>
   3    0003.e386.47f0    DYNAMIC     Gi0/2+Efp66
   3    0009.9b00.dd9d    DYNAMIC     Gi0/2+Efp66
   3    0009.9b01.2d25    DYNAMIC     Gi0/2+Efp66
   3    000c.2925.7d4d    DYNAMIC     Gi0/2+Efp66
   3    000c.299b.b392    DYNAMIC     Gi0/2+Efp66
   3    000c.29d8.3445    DYNAMIC     Gi0/2+Efp66
   3    000e.0c9c.3af4    DYNAMIC     Gi0/2+Efp66
   3    000e.0ca8.44c8    DYNAMIC     Gi0/2+Efp66
   3    000e.0cab.2012    DYNAMIC     Gi0/2+Efp66
   3    000e.0cb8.88d1    DYNAMIC     Gi0/2+Efp66
   3    0011.1195.1574    DYNAMIC     Gi0/2+Efp66
   3    0011.1195.157c    DYNAMIC     Gi0/2+Efp66
   3    0011.11f1.ee7c    DYNAMIC     Gi0/2+Efp66
   3    0011.929c.5f58    DYNAMIC     Gi0/2+Efp66
   3    0014.c23b.3573    DYNAMIC     Gi0/2+Efp66
   3    0015.600e.cffe    DYNAMIC     Gi0/2+Efp66
   3    0016.7620.e292    DYNAMIC     Gi0/2+Efp66
   3    0016.7620.f23c    DYNAMIC     Gi0/2+Efp66
   3    0019.563f.4700    DYNAMIC     Gi0/2+Efp66
<output truncated>
Total Mac Addresses for this criterion: 129
```

Related Commands

Command	Description
clear mac address-table dynamic	Deletes from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table interface

To display the MAC address table information for the specified interface in the specified VLAN, use the **show mac address-table interface** command in user EXEC mode.

show mac address-table interface *interface-id* [**vlan** *vlan-id*] [**|** {**begin | exclude | include**} *expression*]

Syntax Description

interface-id	Specifies an interface type; valid interfaces include physical ports and port channels.
vlan *vlan-id*	(Optional) Displays entries for a specific VLAN; the range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table interface** command:

```
Switch> show mac address-table interface gigabitethernet0/2
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0030.b635.7862  DYNAMIC Gi0/2
   1    00b0.6496.2741  DYNAMIC Gi0/2
Total Mac Addresses for this criterion: 2
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table learning

To display the status of MAC address learning for all VLANs and bridge domains or the specified VLAN or bridge domain, use the **show mac address-table learning** command in user EXEC mode.

show mac address-table learning [**bridge-domain** *number*] [**vlan** *vlan-id*] [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

bridge-domain *number*	(Optional) Displays information for a specific Ethernet Flow Point bridge domain. The range is 1 to 8000.
vlan *vlan-id*	(Optional) Displays information for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use the **show mac address-table learning** command without any keywords to display configured VLANs or bridge domains and whether MAC address learning is enabled or disabled on them. The default is that MAC address learning is enabled on all VLANs and bridge domains. Use the command with a specific VLAN ID or bridge domain number to display the learning status on an individual VLAN or bridge domain.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table learning** user EXEC command showing that MAC address learning is disabled on VLAN 200:

```
Switch> show mac address-table learning
VLAN    Learning Status
----    ---------------
1             yes
100           yes
200           no
```

Related Commands

Command	Description
mac address-table learning	Configures MAC address learning on a VLAN or bridge domain.

show mac address-table move update

To display the MAC address-table move update information on the switch, use the **show mac address-table move update** command in user EXEC mode.

show mac address-table move update [| {**begin** | **exclude** | **include**} **expression**]

Syntax Description

| begin	(Optional) Display begins with the line that matches the expression.
| exclude	(Optional) Display excludes lines that match the expression.
| include	(Optional) Display includes lines that match the specified expression.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain output do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table move update** command:

```
Switch> show mac address-table move update
Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

Related Commands

Command	Description
clear mac address-table move update	Clears the MAC address-table move update counters.
mac address-table move update {**receive** | **transmit**}	Configures MAC address-table move update on the switch.

show mac address-table notification

To display the MAC address notification settings for all interfaces or the specified interface, use the **show mac address-table notification** command in user EXEC mode.

show mac address-table notification {**change** [**interface** [*interface-id*] | **mac-move** | **threshold**} [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

change	Displays the MAC change notification feature parameters and the history table.
interface	(Optional) Displays information for all interfaces. Valid interfaces include physical ports and port channels.
interface-id	(Optional) Displays information for the specified interface. Valid interfaces include physical ports and port channels.
mac-move	Displays status for MAC address move notifications.
threshold	Displays status for MAC-address table threshold monitoring.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use the **show mac address-table notification change** command without keywords to see if the MAC address change notification feature is enabled or disabled, the MAC notification interval, the maximum number of entries allowed in the history table, and the history table contents.

Use the **interface** keyword to display the notifications for all interfaces. If the *interface-id* is included, only the flags for that interface appear.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table notification change** command:

```
Switch> show mac address-table notification change
MAC Notification Feature is Enabled on the switch
Interval between Notification Traps : 60 secs
Number of MAC Addresses Added : 4
Number of MAC Addresses Removed : 4
Number of Notifications sent to NMS : 3
Maximum Number of entries configured in History Table : 100
```

```
Current History Table Length : 3
MAC Notification Traps are Enabled
History Table contents
----------------------
History Index 0, Entry Timestamp 1032254, Despatch Timestamp 1032254
MAC Changed Message :
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0001 Module: 0   Port: 1

History Index 1, Entry Timestamp 1038254, Despatch Timestamp 1038254
MAC Changed Message :
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0000 Module: 0   Port: 1
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0002 Module: 0   Port: 1
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0003 Module: 0   Port: 1

History Index 2, Entry Timestamp 1074254, Despatch Timestamp 1074254
MAC Changed Message :
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0000 Module: 0   Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0001 Module: 0   Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0002 Module: 0   Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0003 Module: 0   Port: 1
```

Related Commands

Command	Description
clear mac address-table notification	Clears the MAC address notification global counters.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table static	Displays static MAC address table entries only.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table static

To display only static MAC address table entries, use the **show mac address-table static** command in user EXEC mode.

show mac address-table static [**address** *mac-address*] [**bridge-domain** *number*] [**interface** *interface-id*] [**vlan** *vlan-id*]
[| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

address *mac-address*	(Optional) Specifies a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only).
bridge-domain *number*	(Optional) Displays information for a specific Ethernet Flow Point bridge domain. The range is 1 to 8000.
interface *interface-id*	(Optional) Displays addresses for a specific interface. Valid interface include physical ports and port channels.
vlan *vlan-id*	(Optional) Displays addresses for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table static** command:

```
Switch> show mac address-table static
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
 All    0100.0ccc.cccc  STATIC  CPU
 All    0180.c200.0000  STATIC  CPU
 All    0100.0ccc.cccd  STATIC  CPU
 All    0180.c200.0001  STATIC  CPU
 All    0180.c200.0004  STATIC  CPU
 All    0180.c200.0005  STATIC  CPU
   4    0001.0002.0004  STATIC  Drop
   6    0001.0002.0007  STATIC  Drop
Total Mac Addresses for this criterion: 8
```

Related Commands

Command	Description
mac address-table static	Adds static addresses to the MAC address table.
mac address-table static drop	Enables unicast MAC address filtering and configures the switch to drop traffic with a specific source or destination MAC address.
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table vlan	Displays the MAC address table information for the specified VLAN.

show mac address-table vlan

To display the MAC address table information for the specified VLAN, use the **show mac address-table vlan** command in user EXEC mode.

show mac address-table vlan *vlan-id* [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

vlan-id	(Optional) Displays addresses for a specific VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show mac address-table vlan 1** command:

```
Switch> show mac address-table vlan 1
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0100.0ccc.cccc  STATIC  CPU
   1    0180.c200.0000  STATIC  CPU
   1    0100.0ccc.cccd  STATIC  CPU
   1    0180.c200.0001  STATIC  CPU
   1    0180.c200.0002  STATIC  CPU
   1    0180.c200.0003  STATIC  CPU
   1    0180.c200.0005  STATIC  CPU
   1    0180.c200.0006  STATIC  CPU
   1    0180.c200.0007  STATIC  CPU
Total Mac Addresses for this criterion: 9
```

Related Commands

Command	Description
show mac address-table address	Displays MAC address table information for the specified MAC address.
show mac address-table aging-time	Displays the aging time in all VLANs or the specified VLAN.
show mac address-table count	Displays the number of addresses present in all VLANs or the specified VLAN.
show mac address-table dynamic	Displays dynamic MAC address table entries only.
show mac address-table interface	Displays the MAC address table information for the specified interface.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or the specified interface.
show mac address-table static	Displays static MAC address table entries only.

show network-clocks

To display information about Synchronous Ethernet (SyncE) clock configuration for the switch, use the **show network-clocks** command in privileged EXEC mode.

show network-clocks [**|** {**begin | exclude | include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC -

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show networks-clocks** command:

```
Switch# show network-clocks

Network Clock Configuration
Input Clock BITS: invalid
Input Clock SYNCE Te0/1: valid
Input Clock SYNCE Te0/2 : valid
System Clock Lock Status (T0DPLL) : Free Run
Output Clock Generated from T4 DPLL
T4 DPLL Lock Status : Not Locked
System Clock Selected Ref: None
T4 DPLL Selected Ref: None
System Clock (T0 DPLL) Info:
Priority  Source            Type

------------------------------------------------------------

 T4 DPLL Clock Info:
Priority  Source            Type

------------------------------------------------------------

------------------------------------------------------------

System Clock Mode : Revertive

 EEC Option Configured : Option 1
```

```
System Clock State is Automatic

------------------------------------------------------------------

 hold-timeout : infinite
 ESMC/SSM workaround using REP not configured

------------------------------------------------------------------
Measured offset freq for input BITS is +483.87ppm (3.8 ppm resolution)
Measured offset freq for input Te0/1 is +0.0ppm (3.8 ppm resolution)
Measured offset freq for input Te0/2 is +0.0ppm (3.8 ppm resolution)
Measured offset freq for current path (T4 DPLL) is Not Available
```

Related Commands

Command	Description
network-clock-select	Configures the network clock for the switch..
set network-clocks	Set SyncE clock selection on the switch.

show pagp

To display Port Aggregation Protocol (PAgP) channel-group information, use the **show pagp** command in user EXEC mode.

show pagp [*channel-group-number*] {**counters** | **internal** | **neighbor**} [| {**begin** | **exclude** | **include**} *expression*]]

Syntax Description

channel-group-number	(Optional) Number of the channel group. The range is 1 to 26.
counters	Displays PAgP traffic information.
internal	Displays PAgP internal information.
neighbor	Displays PAgP neighbor information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can enter any **show pagp** command to display the active channel-group information. To display the nonactive information, enter the **show pagp** command with a channel-group number.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* are appear.

Examples

This is an example of output from the **show pagp 1 counters** command:

```
Switch> show pagp 1 counters
             Information        Flush
Port         Sent   Recv     Sent   Recv
---------------------------------------
Channel group: 1
Gi0/1      45     42       0      0
  Gi0/2      45     41       0      0
```

This is an example of output from the **show pagp 1 internal** command:

```
Switch> show pagp 1 internal
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Channel group 1
                                Hello    Partner  PAgP     Learning  Group
Port        Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi0/1       SC    U6/S7   H       30s      1        128        Any      16
Gi0/2       SC    U6/S7   H       30s      1        128        Any      16
```

This is an example of output from the **show pagp 1 neighbor** command:

```
Switch> show pagp 1 neighbor
   Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
           A - Device is in Auto mode.        P - Device learns on physical port.

   Channel group 1 neighbors
             Partner             Partner          Partner           Partner Group
   Port      Name                Device ID        Port         Age  Flags   Cap.
   Gi0/1     switch-p2           0002.4b29.4600   Gi0/1          9s SC      10001
   Gi0/2     switch-p2           0002.4b29.4600   Gi0/2         24s SC      10001
```

Related Commands

Command	Description
clear pagp	Clears PAgP channel-group information.

show parser macro

To display the parameters for all configured macros or for one macro on the switch, use the **show parser macro** command in user EXEC mode.

show parser macro [{**brief** | **description** [**interface** *interface-id*] | **name** *macro-name*}] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

brief	(Optional) Displays the name of each macro.
description [**interface** *interface-id*]	(Optional) Displays all macro descriptions or the description of a specific interface.
name *macro-name*	(Optional) Displays information about a single macro identified by the macro name.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is a partial output example from the **show parser macro** command:

```
Switch# show parser macro
Total number of macros = 2
------------------------------------------------------------------
Macro name : sample-macro1
Macro type : customizable
duplex full
speed auto
mdix auto
------------------------------------------------------------------
Macro name : test1
Macro type : customizable
no shutdown
flowcontrol receive on
speed 100
------------------------------------------------------------------
```

This is an example of output from the **show parser macro name** command:

```
Switch# show parser macro name sample-macro1
Macro name : sample-macro1
Macro type : customizable
duplex full
speed auto
mdix auto
```

This is an example of output from the **show parser macro brief** command:

```
Switch# show parser macro brief
    customizable     : sample-macro1
    customizable     : test1
```

Related Commands

Command	Description
macro apply	Applies a macro on an interface or applies and traces a macro on an interface.
macro description	Adds a description about the macros that are applied to an interface.
macro global	Applies a macro on a switch or applies and traces a macro on a switch.
macro global description	Adds a description about the macros that are applied to the switch.
macro name	Creates a macro.
show running-config	Displays the operating configuration.

show policy-map

To display quality of service (QoS) policy maps, which define classification criteria for incoming and outgoing traffic and the actions to be performed on the classified traffic, use the **show policy-map** command in user EXEC mode.

show policy-map [*policy-map-name* | **control-plane** [**all**] | **interface** [*interface-id*]] [**input** | **output**] [**class** *class-name*] | [**service instance** *number*]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

policy-map-name	(Optional) Displays the specified policy-map name.
control-plane [**all**]	(Optional) Displays the control plane policy or all control plane policies.
interface [*interface-id*]	(Optional) Displays information and statistics about policy maps applied to all ports or the specified port. • *interface-id*—Displays information about policy maps on the specified physical interface.
[**input** | **output**]	(Optional) If you specify control plane or a port, you can specify additional keywords.The keywords have these meanings: • **input**—Displays information about input policy maps on the switch or applied to the specified port. • **output**—Displays information about output policy-maps on the switch or applied to the specified port.
class *class-name*	(Optional) Displays policy-map statistics for an individual class.
service instance *number*	(Optional) Displays policy map information for a service instance. The service instance number range is from 1 to 4294967295.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of the output of the **show policy-map interface** command showing statistics for an output policy map.

```
Switch# show policy-map interface gigabitethernet 0/2
 GigabitEthernet0/2

  Service-policy output: phb

    Class-map: phb (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: cos  2
          Bandwidth 1000 (kbps)
          Queue-limit current-queue-depth 0 bytes
              Output Queue:
                Tail Packets Drop: 0
                Tail Bytes Drop: 0

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

This is an example of output from the **show policy-map** command for a specific policy map:

```
Switch> show policy-map top2
  Policy Map top2
    Class class-default
      shape average 11111124
      service-policy pout
```

This is an example of output from the **show policy-map** command for an output policy map:

```
Switch> show policy-map pout
  Policy Map pout
    Class ip1
      priority
     police cir percent 10
       conform-action transmit
       exceed-action drop
      queue-limit 250
      queue-limit precedence  1 100
    Class ip2
      Average Rate Traffic Shaping
      cir 5%
    Class ip3
      bandwidth percent 10
      queue-limit 200
      queue-limit precedence  3 100
```

This is an example of output from the **show policy-map** command for an input policy map:

```
Switch> show policy-map pin-police
Policy Map pin-police
    Class ip1
     police cir 20000000 bc 625000
       conform-action transmit
       exceed-action drop
       violate-action drop
```

Table 2-18 describes the fields in the **show policy-map interface** display. The fields in the table are grouped according to the relevant QoS feature.

Table 3-14 show policy-map interface Field Descriptions

Field	Description
Fields associated with classes or service policies	
Service-policy input/output	Name of the input or output service policy applied to the specified interface.
Class-map	Class of traffic shown. Output appears for each configured class in the policy. The choice for implementing class matches (match-all or match-any) might also appear next to the traffic class.
packets	Number of packets identified as belonging to the traffic class.
Match	Match criteria specified for the class of traffic. This includes criteria such as class of service (CoS) value, discard class, IP precedence value, multiprotocol label switching (MPLS) experimental (EXP) value, Differentiated Services Code Point (DSCP) value, access groups, and QoS groups.
Fields associated with policing	
police	Shown when the **police** command has been configured to enable traffic policing. Displays the specified committed information rate (CIR) and conform burst size (BC) used for policing packets.
conform-action	Displays the action to be taken on packets marked as conforming to a specified rate.
conform	Displays the number of packets marked as conforming to the specified rate.
exceed-action	Displays the actions to be taken on packets marked as exceeding a specified rate.
exceed	Displays the number of packets marked as exceeding the specified rate.
violate-action	Displays the actions to be taken on packets marked as exceeding the maximum rate.
violate	Displays the number of packets marked as exceeding the maximum rate.
Fields associated with queuing	
Queue Limit	Queue size configured for the class in number of packets.
Output Queue	The queue created for this class of traffic.
Tail packets dropped	The number of packets dropped when the mean queue depth is greater than the maximum threshold value.
Fields associated with traffic scheduling	
Traffic shaping	The rate used for shaping traffic.
Bandwidth	Bandwidth configured for this class in kbps or a percentage.
Priority	Indicates that this class is configured for priority queuing.

Related Commands

Command	Description
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.

show port-type

To display interface type information for the Cisco ME switch, use the **show port-type** command in privileged EXEC mode.

show port-type [**eni** | **nni** | **uni**] [| {**begin** | **exclude** | **include**} *expression*]

Note All ports on the switch are network node interfaces (NNIs), so only **nni** output is valid.

Syntax Description

eni	Enhanced network interface.
nni	Network node interface.
uni	User network interface.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If you enter the command without keywords, the output includes the interface type information for all ports on the switch. If you specify the port type (**eni**, **nni**, or **uni**), the output includes information for the specified port type.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show port-type** command. The output is the same for **show port-type** and s**how port-type nni**:

```
Switch# show port-type nni
Port      Name               Vlan       Port Type
--------- ------------------ ---------- ----------------------------
Gi0/1                        trunk      Network Node Interface           (nni)
Gi0/2                        trunk      Network Node Interface           (nni)
Gi0/3                        trunk      Network Node Interface           (nni)
Gi0/4                        1          Network Node Interface           (nni)
Gi0/5                        1          Network Node Interface           (nni)
Gi0/6                        routed     Network Node Interface           (nni)
Gi0/7                        1          Network Node Interface           (nni)
Gi0/8                        1          Network Node Interface           (nni)
Gi0/9                        1          Network Node Interface           (nni)
```

```
Gi0/10                       1          Network Node Interface           (nni)
Gi0/11    testwhelshdevice   1          Network Node Interface           (nni)
Gi0/12                       1          Network Node Interface           (nni)
Gi0/13                       trunk      Network Node Interface           (nni)
Gi0/14                       1          Network Node Interface           (nni)
Gi0/15                       1          Network Node Interface           (nni)
Gi0/16                       1          Network Node Interface           (nni)
Gi0/17                       1          Network Node Interface           (nni)
Gi0/18                       1          Network Node Interface           (nni)
Gi0/19                       1          Network Node Interface           (nni)
Gi0/20                       1          Network Node Interface           (nni)
Gi0/21                       1          Network Node Interface           (nni)
Gi0/22                       1          Network Node Interface           (nni)
Gi0/23                       1          Network Node Interface           (nni)
Gi0/24                       1          Network Node Interface           (nni)
Te0/1                        1          Network Node Interface           (nni)
Te0/2                        1          Network Node Interface           (nni)
```

This is an example of output from the **show port-type** command using other keywords:

```
Switch# show port-type nni | exclude Gigabitethernet0/1
Port      Name               Vlan       Port Type
--------- ------------------ ---------- ----------------------------
Gi0/2                        1          Network Node Interface (nni)
```

Related Commands

Command	Description
port-type	Sets the interface type for a port, but all ports are NNIs.

show rep topology

To display Resilient Ethernet Protocol (REP) topology information for a segment or for all segments, including the primary and secondary edge ports in the segment., use the **show rep topology** command in user EXEC mode.

show rep topology [**segment** *segment_id*] [**archive**] [**detail**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

segment-id	(Optional) Displays REP topology information for the specified segment. The ID range is from 1 to 1024.
archive	(Optional) Displays the previous topology of the segment. This keyword can be useful for troubleshooting a link failure.
detail	(Optional) Displays detailed REP topology information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

In the **show rep topology** command output, ports configured as edge no-neighbor are designated with an asterisk (*) in front of *Pri* or *Sec*. In the output of the **show rep topology detail** command, *No-Neighbor* is spelled out.

The output of this command is also included in the **show tech-support** privileged EXEC command output.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is a sample output from the **show rep topology segment** privileged EXEC command:

```
Switch # show rep topology segment 1
REP Segment 1
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
sw1_multseg_3750 Gi1/1/1    Pri  Alt
sw3_multseg_3400 Gi0/13          Open
sw3_multseg_3400 Gi0/14          Alt
sw4_multseg_3400 Gi0/13          Open
sw4_multseg_3400 Gi0/14          Open
sw5_multseg_3400 Gi0/13          Open
```

```
sw5_multseg_3400 Gi0/14          Open
sw2_multseg_3750 Gi1/1/2         Open
sw2_multseg_3750 Gi1/1/1         Open
sw1_multseg_3750 Gi1/1/2    Sec  Open
```

This is a sample output from the **show rep topology** command when the edge ports are configured to have no REP neighbor:

```
Switch # show rep topology
REP Segment 2
BridgeName       PortName   Edge  Role
---------------- ---------- ----  ----
sw8-ts8-51       Gi0/2      Pri*  Open
sw9-ts11-50      Gi1/0/4          Open
sw9-ts11-50      Gi1/0/2          Open
sw1-ts11-45      Gi0/2            Alt
sw1-ts11-45      Po1              Open
sw8-ts8-51       Gi0/1      Sec*  Open
```

This example shows output from the **show rep topology detail** command:

```
Switch# show rep topology detail
REP Segment 2
repc_2_24ts, Fa0/2 (Primary Edge)
  Alternate Port, some vlans blocked
  Bridge MAC: 0019.e714.5380
  Port Number: 004
  Port Priority: 080
  Neighbor Number: 1 / [-10]
repc_3_12cs, Gi0/1 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a292.3580
  Port Number: 001
  Port Priority: 000
  Neighbor Number: 2 / [-9]
repc_3_12cs, Po10 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a292.3580
  Port Number: 080
  Port Priority: 000
  Neighbor Number: 3 / [-8]
repc_4_12cs, Po10 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 001a.a19d.7c80
  Port Number: 080
  Port Priority: 000
  Neighbor Number: 4 / [-7]
repc_4_12cs, Gi0/2 (Intermediate)
  Alternate Port, some vlans blocked
  Bridge MAC: 001a.a19d.7c80
  Port Number: 002
  Port Priority: 040
  Neighbor Number: 5 / [-6]

<output truncated>
```

This example shows output from the **show rep topology segment archive** command:

```
Switch# show rep topology segment 1 archive
REP Segment 1
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
sw1_multseg_3750 Gi1/1/1    Pri  Open
sw3_multseg_3400 Gi0/13          Open
sw3_multseg_3400 Gi0/14          Open
sw4_multseg_3400 Gi0/13          Open
sw4_multseg_3400 Gi0/14          Open
sw5_multseg_3400 Gi0/13          Open
sw5_multseg_3400 Gi0/14          Open
sw2_multseg_3750 Gi1/1/2         Alt
sw2_multseg_3750 Gi1/1/1         Open
sw1_multseg_3750 Gi1/1/2    Sec  Open
```

Related Commands

Command	Description
rep segment	Enables REP on an interface and assigns a segment ID. This command is also used to configure a port as an edge port, a primary edge port, or a preferred port.

show spanning-tree

To display spanning-tree state information, use the **show spanning-tree** command in user EXEC mode.

show spanning-tree [*bridge-group* | **active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **mst** | **pathcost method** | **root** | **summary** [**totals**] | **vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree *bridge-group* [**active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **root** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree vlan *vlan-id* [**active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **root** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree {**vlan** *vlan-id* | *bridge-group*} **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree {**vlan** *vlan-id* | *bridge-group*} **root** [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree interface *interface-id* [**active** [**detail**] | **cost** | **detail** [**active**] | **inconsistency** | **portfast** | **priority** | **rootcost** | **state**] [| {**begin** | **exclude** | **include**} *expression*]

show spanning-tree mst [**configuration [digest**]] | [*instance-id* [**detail** | **interface** *interface-id* [**detail**]] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

bridge-group	(Optional) Specify the bridge group number. The range is 1 to 255.
active [**detail**]	(Optional) Display spanning-tree information only on active interfaces (available only in privileged EXEC mode).
blockedports	(Optional) Display blocked port information (available only in privileged EXEC mode).
bridge [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**]	(Optional) Display status and configuration of this switch (optional keywords available only in privileged EXEC mode).
detail [**active**]	(Optional) Display a detailed summary of interface information (**active** keyword available only in privileged EXEC mode).
inconsistentports	(Optional) Display inconsistent port information (available only in privileged EXEC mode).
interface *interface-id* [**active** [**detail**] | **cost** | **detail** [**active**] | **inconsistency** | **portfast** | **priority** | **rootcost** | **state**]	(Optional) Display spanning-tree information for the specified interface (all options except **portfast** and **state** available only in privileged EXEC mode). Enter each interface separated by a space. Ranges are not supported. Valid interfaces include physical interfaces and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 26.

mst [**configuration** [**digest**]] [*instance-id* [**detail** | **interface** *interface-id* [**detail**]]	(Optional) Display the multiple spanning-tree (MST) region configuration and status (available only in privileged EXEC mode). The keywords have these meanings: • **digest**—(Optional) Display the MD5 digest included in the current MST configuration identifier (MSTCI). Two separate digests, one for standard and one for prestandard switches, appear (available only in privileged EXEC mode). The terminology was updated for the implementation of the IEEE standard, and the *txholdcoun*t field was added. The new master role appears for boundary ports. The word *pre-standard* or *Pre-STD* appears when an IEEE standard bridge sends prestandard BPDUs on a port. The word *pre-standard (config)* or *Pre-STD-Cf* appears when a port has been configured to send prestandard BPDUs and no prestandard BPDU has been received on that port. The word *pre-standard (rcvd)* or *Pre-STD-Rx* appears when a prestandard BPDU has been received on a port that has not been configured to send prestandard BPDUs. A *dispute* flag appears when a designated port receives inferior designated information until the port returns to the forwarding state or ceases to be designated. • *instance-id*—You can specify a single instance ID, a range of IDs separated by a hyphen, or a series of IDs separated by a comma. The range is 1 to 4094. The display shows the number of currently configured instances. • **interface** *interface-id*—(Optional) Valid interfaces include VLANs, physical interfaces, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 26. • **detail**—(Optional) Display detailed information for the instance or interface.
pathcost method	(Optional) Display the default path cost method (available only in privileged EXEC mode).
root [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**]]	(Optional) Display root switch status and configuration (all keywords available only in privileged EXEC mode).
summary [**totals**]	(Optional) Display a summary of port states or the total lines of the spanning-tree state section.
vlan *vlan-id* [**active** [**detail**] | **backbonefast** | **blockedports** | **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**]	(Optional) Display spanning-tree information for the specified VLAN (some keywords available only in privileged EXEC mode). You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.

| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If the *vlan-id* variable is omitted, the command applies to the spanning-tree instance for all VLANs.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show spanning-tree active** command:

```
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0001.42e2.cdd0
             Cost        3038
             Port        24 (GigabitEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    49153  (priority 49152 sys-id-ext 1)
             Address     0003.fd63.9580
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
  Uplinkfast enabled

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Root FWD 3019      128.24   P2p
<output truncated>
```

This is an example of output from the **show spanning-tree detail** command:

```
Switch# show spanning-tree detail
VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 49152, sysid 1, address 0003.fd63.9580
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0001.42e2.cdd0
  Root port is 24 (GigabitEthernet0/1), cost of root path is 3038
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 1d16h ago
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300
  Uplinkfast enabled

 Port 1 (GigabitEthernet0/1) of VLAN0001 is forwarding
   Port path cost 3019, Port priority 128, Port Identifier 128.24.
```

```
   Designated root has priority 32768, address 0001.42e2.cdd0
   Designated bridge has priority 32768, address 00d0.bbf5.c680
   Designated port id is 128.25, designated path cost 19
   Timers: message age 2, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 0, received 72364
<output truncated>
```

This is an example of output from the **show spanning-tree interface** *interface-id* command:

```
Switch# show spanning-tree interface gigabitethernet0/1
Vlan             Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Root FWD 3019      128.24   P2p
```

This is an example of output from the **show spanning-tree summary** command:

```
Switch# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID   is enabled
Portfast             is disabled by default
PortFast BPDU Guard  is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard            is disabled by default
Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                  1        0         0        11         12
VLAN0002                  3        0         0        1          4
VLAN0004                  3        0         0        1          4
VLAN0006                  3        0         0        1          4
VLAN0031                  3        0         0        1          4
VLAN0032                  3        0         0        1          4
<output truncated>
---------------------- -------- --------- -------- ---------- ----------
37 vlans                  109      0         0        47         156
Station update rate set to 150 packets/sec.
```

This is an example of output from the **show spanning-tree mst configuration** command:

```
Switch# show spanning-tree mst configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
--------  ------------------
0         1-9,21-4094
1         10-20
----------------------------
```

This is an example of output from the **show spanning-tree mst configuration digest** command:

```
Switch# show spanning-tree mst configuration
% Switch is not in mst mode
Name      []
Revision  0     Instances configured 1
Digest          0xAC36177F50283CD4B83821D8AB26DE62
Pre-std Digest  0xBB3B6C15EF8D089BB55ED10D24DF44DE
```

This is an example of output from the **show spanning-tree mst interface** *interface-id* command:

```
Switch# show spanning-tree mst interface gigabitethernet0/1
GigabitEthernet0/1 of MST00 is root forwarding
Edge port: no             (default)        port guard : none        (default)
Link type: point-to-point (auto)           bpdu filter: disable     (default)
Boundary : boundary       (STP)            bpdu guard : disable     (default)
Bpdus sent 5, received 74

Instance role state cost      prio vlans mapped
0        root FWD   200000    128  1,12,14-4094
```

This is an example of output from the **show spanning-tree mst 0** command:

```
Switch# show spanning-tree mst 0
###### MST00        vlans mapped: 1-9,21-4094
Bridge      address 0002.4b29.7a00  priority  32768 (32768 sysid 0)
Root        address 0001.4297.e000  priority  32768 (32768 sysid 0)
port    Gi0/1           path cost 200038
IST master *this switch
Operational hello time 2, forward delay 15, max age 20, max hops 20
Configured  hello time 2, forward delay 15, max age 20, max hops 20

Interface              role state cost      prio type
---------------------  ---- ----- --------- ---- --------------------------------
GigabitEthernet0/1     root FWD   200000    128  P2P bound(STP)
GigabitEthernet0/2     desg FWD   200000    128  P2P bound(STP)
Port-channel1          desg FWD   200000    128  P2P bound(STP)
```

Related Commands

Command	Description
clear spanning-tree counters	Clears the spanning-tree counters.
clear spanning-tree detected-protocols	Restarts the protocol migration process.
spanning-tree bpdufilter	Prevents an interface from sending or receiving bridge protocol data units (BPDUs).
spanning-tree bpduguard	Puts an interface in the error-disabled state when it receives a BPDU.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree extend system-id	Enables the extended system ID feature.
spanning-tree guard	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
spanning-tree link-type	Overrides the default link-type setting for rapid spanning-tree transitions to the forwarding state.
spanning-tree loopguard default	Prevents alternate or root ports from becoming the designated port because of a failure that leads to a unidirectional link.
spanning-tree mst configuration	Enters multiple spanning-tree (MST) configuration mode through which the MST region configuration occurs.
spanning-tree mst cost	Sets the path cost for MST calculations.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.

Command	Description
spanning-tree mst max-hops	Sets the number of hops in an MST region before the BPDU is discarded and the information held for an interface is aged.
spanning-tree mst port-priority	Configures an interface priority.
spanning-tree mst priority	Configures the switch priority for the specified spanning-tree instance.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree port-priority	Configures an interface priority.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an interface and all its associated VLANs.
spanning-tree vlan	Configures spanning tree on a per-VLAN basis.

show storm-control

To display broadcast, multicast, or unicast storm control settings on the switch or on the specified interface, or to display storm-control history, use the **show storm-control** command in user EXEC mode.

show storm-control [*interface-id*] [**broadcast** | **multicast** | **unicast**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) Interface ID for the physical port (including type, module, and port number).
broadcast	(Optional) Displays broadcast storm threshold setting.
multicast	(Optional) Displays multicast storm threshold setting.
unicast	(Optional) Displays unicast storm threshold setting.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When you enter an *interface-id*, the storm control thresholds appear for the specified interface.

If you do not enter an *interface-id*, settings appear for one traffic type for all ports on the switch.

If you do not enter a traffic type, settings appear for broadcast storm control.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of a partial output from the **show storm-control** command when no keywords are entered. Because no traffic-type keyword was entered, the broadcast storm control settings appear.

```
Switch> show storm-control
Interface    Filter State   Upper       Lower      Current
---------    -------------  ----------  ---------  ---------
Gi0/1        Forwarding     20 pps      10 pps     5 pps
Gi0/2        Forwarding     50.00%      40.00%     0.00%
<output truncated>
```

This is an example of output from the **show storm-control** command for a specified interface. Because no traffic-type keyword was entered, the broadcast storm control settings appear.

```
Switch> show storm-control gigabitethernet 0/1
Interface    Filter State   Upper       Lower      Current
---------    -------------  ----------  ---------  ---------
Gi0/1        Forwarding     20 pps      10 pps     5 pps
```

Table 2-19 describes the fields in the **show storm-control** display.

Table 3-15 show storm-control Field Descriptions

Field	Description
Interface	Displays the ID of the interface.
Filter State	Displays the status of the filter: • Blocking—Storm control is enabled, and a storm has occurred. • Forwarding—Storm control is enabled, and no storms have occurred. • Inactive—Storm control is disabled.
Upper	Displays the rising suppression level as a percentage of total available bandwidth in packets per second or in bits per second.
Lower	Displays the falling suppression level as a percentage of total available bandwidth in packets per second or in bits per second.
Current	Displays the bandwidth usage of broadcast traffic or the specified traffic type (broadcast, multicast, or unicast) as a percentage of total available bandwidth. This field is only valid when storm control is enabled.

Related Commands

Command	Description
storm-control	Sets the broadcast, multicast, or unicast storm control levels for the switch.

show udld

To display UniDirectional Link Detection (UDLD) administrative and operational status for all ports or the specified port, use the **show udld** command in user EXEC mode.

show udld [*interface-id*] [**neighbors**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

interface-id	(Optional) ID of the interface and port number. Valid interfaces include physical ports and VLANs. The VLAN range is 1 to 4094.
neighbors	(Optional) Displays a summary of UDLD neighbors.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If you do not enter an *interface-id*, administrative and operational UDLD status for all interfaces appear.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show udld** *interface-id* command. For this display, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. Table 2-20 describes the fields in this display.

```
Switch> show udld gigabitethernet0/1
Interface gi0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
    Entry 1
    Expiration time: 146
    Device ID: 1
    Current neighbor state: Bidirectional
    Device name: Switch-A
    Port ID: Gi0/1
    Neighbor echo 1 device: Switch-B
    Neighbor echo 1 port: Gi0/2
    Message interval: 5
    CDP Device name: Switch-A
```

Table 3-16 show udld Field Descriptions

Field	Description
Interface	The interface on the local device configured for UDLD.
Port enable administrative configuration setting	How UDLD is configured on the port. If UDLD is enabled or disabled, the port enable configuration setting is the same as the operational enable state. Otherwise, the enable operational setting depends on the global enable setting.
Port enable operational state	Operational state that shows whether UDLD is actually running on this port.
Current bidirectional state	The bidirectional state of the link. An unknown state appears if the link is down or if it is connected to an UDLD-incapable device. A bidirectional state appears if the link is a normal two-way connection to a UDLD-capable device. All other values mean miswiring.
Current operational state	The current phase of the UDLD state machine. For a normal bidirectional link, the state machine is most often in the Advertisement phase.
Message interval	How often advertisement messages are sent from the local device. Measured in seconds.
Time out interval	The time period, in seconds, that UDLD waits for echoes from a neighbor device during the detection window.
Entry 1	Information from the first cache entry, which contains a copy of echo information received from the neighbor.
Expiration time	The amount of time in seconds remaining before this cache entry is aged out.
Device ID	The neighbor device identification.
Current neighbor state	The neighbor's current state. If both the local and neighbor devices are running UDLD normally, the neighbor state and local state should be bidirectional. If the link is down or the neighbor is not UDLD-capable, no cache entries appear.
Device name	The device name or the system serial number of the neighbor. The system serial number appears if the device name is not set or is set to the default (Switch).
Port ID	The neighbor port ID enabled for UDLD.
Neighbor echo 1 device	The device name of the neighbors' neighbor from which the echo originated.
Neighbor echo 1 port	The port number ID of the neighbor from which the echo originated.
Message interval	The rate, in seconds, at which the neighbor is sending advertisement messages.
CDP device name	The CDP device name or the system serial number. The system serial number appears if the device name is not set or is set to the default (Switch).

Related Commands

Command	Description
udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command.
udld reset	Resets all interfaces shutdown by UDLD and permits traffic to begin passing through them again.

show version

To display version information for the switch hardware and firmware, use the **show version** command in user EXEC mode.

show version [**|** {**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show version** command:

Note Though visible in the **show version** output, the *configuration register* information is not supported on the switch.

```
Switch> show version
Cisco IOS Software, ME380x Software (ME380x-UNIVERSAL-M)
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Tue 12-Oct-10 02:19
Image text-base: 0x00003000, data-base: 0x020881B8

ROM: Bootstrap program is WHALES boot loader
BOOTLDR: ME380x Boot Loader (ME380X-HBOOT-M), Version 12.2

Switch uptime is 1 minute
System returned to ROM by power-on
System image file is
"flash:/me380x-universal-mz.122-52.1.127.EY/me380x-universal-mz.122-52.1.127.E
Y.bin"

License Level: MetroAggrServices
License Type: Permanent
Next reload license Level: MetroAggrServices

cisco ME-3800X-24FS-M (PowerPC8572) processor (revision P3) with 1015808K/32760K bytes of
memory.
```

```
Processor board ID FOC1350X0NW
Last reset from power-on
Target IOS Version 12.2(46)EY
1 Virtual Ethernet interface
25 Gigabit Ethernet interfaces
2 Ten Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

1536K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:27:0C:AB:4E:00
Motherboard assembly number     : 73-12068-05
Motherboard serial number       : FOC13490VLP
Model revision number           : P3
Motherboard revision number     : 06
Model number                    : ME-3800X-24FS-M
System serial number            : FOC1350X0NW
Top Assembly Part Number        : 800-31465-01
Top Assembly Revision Number    : 36
Version ID                      : V01

Configuration register is 0xF
```

show vfi

To display information about a virtual forwarding infrastructure (VFI), use the **show vfi** command in user EXEC mode. VFIs are used to implement hierarchical virtual private LAN service (H-VPLS) over a multiprotocol label switching (MPLS) backbone.

show vfi *vfi-name* [**forwarding**] [**|** {**begin | exclude | include**} *expression*]

Syntax Description

vfi-name	Name of the configured VFI.
forwarding	(Optional) Displays the VFI Layer 2 forwarding table.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

User EXEC

Command History

Release	Modification
12.2.(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

Examples

This is an example of output from the **show vfi** command:

```
Switch> show vfi vfitest1
VFI name:vfitest1, state:UP
  Local attachment circuits:
    Vlan666
  Neighbor connected via pseudowires:11.11.11.11
```

This is an example of output from the **show vfi** command with the **forwarding** keyword:

```
Switch> show vfi vfitest1 forwarding
vcid:222, type:ether , local groupid:37, remote groupid:40 (vc is up)
client:Vfi is up, destination:11.11.11.11, Peer LDP Ident:11.11.11.11:0
local label:20, remote label:21, tunnel label:implc-null
outgoing interface:Gi1/1/2, next hop:2.2.2.1
Local MTU:1500, Remote MTU:1500
Remote interface description:Vfi
Packet totals(in/out):10/3375408
byte totals(in/out):1306/276783942
```

Related Commands

Command	Description
l2vfi	Creates a VFI and enters VFI configuration mode.
debug vqpc	Displays VFI error or event debug messages.

show vlan

To display the parameters for all configured VLANs or a specified VLAN, use the **show vlan** command in user EXEC mode.

show vlan [**access-map** | **brief** | **counters** | **dot1q tag native** | **filter** | **id** *vlan-id* | **mtu** | **name** *vlan-name* | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

access-map	See the **show vlan access-map** command.
brief	(Optional) Displays one line for each VLAN with the VLAN name, status, and its ports.
counters	(Optional) Displays VLAN traffic counters for all VLANs.
dot1q tag native	(Optional) Displays the IEEE 802.1Q native VLAN tagging status. This keyword is supported only when the switch is running the metro IP access or metro access image.
filter	See the **show vlan filter** command.
id *vlan-id*	(Optional) Displays information about a single VLAN identified by VLAN ID number. For *vlan-id*, the range is 1 to 4094.
mtu	(Optional) Displays a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN.
name *vlan-name*	(Optional) Displays information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
summary	(Optional) Displays VLAN summary information.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Note Though visible in the command-line help string, the **ifindex**, **private-vlan**, **remote-span**, and **mnit vlan** keywords are not supported.

Command Modes

User EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

In the **show vlan mtu** command output, the MTU_Mismatch column shows whether all the ports in the VLAN have the same MTU. When *yes* appears in this column, it means that the VLAN has ports with different MTUs. Packets that are switched from a port with a larger MTU to a port with a smaller MTU

might be dropped. If the VLAN does not have a switch virtual interface (SVI), the hyphen (-) symbol appears in the SVI_MTU column. If the MTU-Mismatch column displays *yes*, the names of the port with the MinMTU and the port with the MaxMTU appear.

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show vlan** command. Table 2-21 describes the fields in the display.

Note The switch supports only Ethernet VLANs. You can configure parameters for FDDI and Token Ring VLANs and view the results in the vlan.dat file, but these parameters are not supported or used.

```
Switch> show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005    1500  -     -     -      ibm  -      0     0VLAN Name

VLAN Type              Ports
---------- ----------------- ------------------------------------------
```

Table 3-17 show vlan Command Output Fields

Field	Description
VLAN	VLAN number.
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.

Table 3-17 show vlan Command Output Fields (continued)

Field	Description
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB.
Trans1	Translation bridge 1.
Trans2	Translation bridge 2.
Remote SPAN VLANs	Identifies any RSPAN VLANs that have been configured.
Primary/Secondary/ Type/Ports	Includes any configured private VLANs, including the primary VLAN ID, the secondary VLAN ID, the type of secondary VLAN (community or isolated), and the ports that belong to it.
VLAN Type/Ports	Displays any configured UNI-ENI VLANs, the type (community or isolated), and the ports that belong to it.

This is an example of output from the **show vlan dot1q tag native** command:

```
Switch> show vlan dot1q tag native
dot1q native vlan tagging is disabled
```

This is an example of output from the **show vlan mtu** command:

```
Switch> show vlan mtu

VLAN    SVI_MTU    MinMTU(port)      MaxMTU(port)     MTU_Mismatch
---- ------------ ----------------  ---------------  ------------
1    1500         1500              1500              No
```

This is an example of output from the **show vlan summary** command:

```
Switch> show vlan summary
Number of existing VLANs           : 45
 Number of existing VTP VLANs      : 0
 Number of existing extended VLANs : 0
```

This is an example of output from the **show vlan id** command.

```
Switch# show vlan id 2
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    VLAN0200                         active    Gi0/1, Gi0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled
```

Related Commands

Command	Description
switchport mode	Configures the VLAN membership mode of a port.
vlan	Enables VLAN configuration mode where you can configure VLANs 1 to 4094.

show vlan access-map

To display information about a particular VLAN access map or for all VLAN access maps, use the **show vlan access-map** command in privileged EXEC mode.

show vlan access-map [*mapname*] [**|** {**begin | exclude | include**} *expression*]

Syntax Description

mapname	(Optional) Name of a specific VLAN access map.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show vlan access-map** command:

```
Switch# show vlan access-map
Vlan access-map "SecWiz"  10
  Match clauses:
    ip  address: SecWiz_Fa1_0_3_in_ip
  Action:
    forward
```

Related Commands

Command	Description
show vlan filter	Displays information about all VLAN filters or about a particular VLAN or VLAN access map.
vlan access-map	Creates a VLAN map entry for VLAN packet filtering.
vlan filter	Applies a VLAN map to one or more VLANs.

show vlan filter

To display information about all VLAN filters or about a particular VLAN or VLAN access map, use the **show vlan filter** command in privileged EXEC mode.

show vlan filter [**access-map** *name* | **vlan** *vlan-id*] [| {**begin** | **exclude** | **include**} *expression*]

Syntax Description

access-map *name*	(Optional) Displays filtering information for the specified VLAN access map.
vlan *vlan-id*	(Optional) Displays filtering information for the specified VLAN. The range is 1 to 4094.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

Examples

This is an example of output from the **show vlan filter** command:

```
Switch# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```

Related Commands

Command	Description
show vlan access-map	Displays information about a particular VLAN access map or for all VLAN access maps.
vlan access-map	Creates a VLAN map entry for VLAN packet filtering.
vlan filter	Applies a VLAN map to one or more VLANs.

shutdown

To disable an interface or Ethernet flow point (EFP) service instance, use the **shutdown** command in interface configuration or service-instance configuration mode. To restart a disabled interface or service instance, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration or service-instance configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **shutdown** command causes a port or service instance to stop forwarding.

The **no shutdown** command has no effect if the port is a static-access port assigned to a VLAN that has been deleted, suspended, or shut down. The port must first be a member of an active VLAN before it can be re-enabled.

The **shutdown** command disables all functions on the specified interface or service instance.

This command also marks the interface. To see if an interface is disabled, use the **show interfaces** privileged EXEC command. An interface that has been shut down is shown as administratively down in the display.

Examples

These examples show how to disable and re-enable a port and a service instance:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# shutdown

Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no shutdown

Switch (config)# interface gigabitethernet0/1
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# shutdown

Switch (config)# interface gigabitethernet0/1
Switch (config-if)# service instance 1 Ethernet
Switch (config-if-srv)# no shutdown
```

Related Commands

Command	Description
show interfaces	Displays the statistical information for all interfaces or for a specific interface.

shutdown vlan

To shut down (suspend) local traffic on the specified VLAN, use the **shutdown vlan** command in global configuration mode. To restart local traffic on the VLAN, use the **no** form of this command.

shutdown vlan *vlan-id*

no shutdown vlan *vlan-id*

Syntax Description

vlan-id	ID of the VLAN to be locally shut down. The range is 2 to 1001. VLANs defined as default VLANs (1 and 1002 to 1005), as well as extended-range VLANs (greater than 1005) cannot be shut down.

Defaults

No default is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use the shutdown VLAN configuration command to shut down local traffic on any VLAN, including extended-range VLANs (1006-4094).

You can verify your setting by entering the **show vlan** privileged EXEC command.

Examples

This example shows how to shut down traffic on VLAN 2:

```
Switch(config)# shutdown vlan 2
```

Related Commands

Command	Description
shutdown (VLAN configuration)	Shuts down local traffic on the VLAN when in VLAN configuration mode (accessed by the **vlan** *vlan-id* global configuration command).

snmp mib rep trap-rate

To configure the sending of Resilient Ethernet Protocol (REP) SNMP traps when there is a link operational status or port role change, use the **snmp mib rep trap-rate** command in global configuration mode. To disable sending of the REP trap, use the **no** version of the command.

snmp mib rep trap-rate *value*

no snmp mib rep trap-rate

Syntax Description

trap-rate *value*	Sets the number of REP traps sent per second. The range is from 0 to 1000. The default is 0 (no limit imposed; a trap is sent at every occurrence).

Defaults

Sending REP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use this command to enable the switch to send REP specific traps corresponding to link operational status changes and port role changes.

Examples

This example configures the switch to send REP traps at a rate of 10 per second:

```
Switch(config)# snmp mib rep trap-rate 10
```

Related Commands

Command	Description
show running config	Verifies that REP traps are configured.

snmp-server enable traps

To enable the switch to send Simple Network Management Protocol (SNMP) notifications for various traps or inform requests to the network management system (NMS), use the **snmp-server enable traps** command in global configuration mode. To return to the default setting, use the **no** form of this command.

snmp-server enable traps [**alarms** [*severity*] | **auth-framework | bgp | bridge** [**newroot**] [**topologychange**] | **cef | config | copy-config | cpu threshold | entity | envmon** [**fan | shutdown | status | supply | temperature**] | **ethernet | ether oam | flash | hsrp | ipmulticast | mac-notification** [**change**] [**move**] [**threshold**] | **mpls | msdp | ospf** [**cisco-specific | errors | lsa | rate-limit | retransmit | state-change**] | **pim [invalid-pim-message | neighbor-change | rp-mapping-change] | rtr | snmp** [**authentication | coldstart | linkdown | linkup | warmstart**] | **storm-control trap-rate** *value* | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog | transceiver all | tty | vlan-membership | vlancreate | vlandelete**]

no snmp-server enable traps [**alarms** [*severity*] | **auth-framework | bgp | bridge** [**newroot**] [**topologychange**] | **cef | config | copy-config | cpu threshold | entity | envmon** [**fan | shutdown | status | supply | temperature**] | **ethernet | ether oam | flash | hsrp | ipmulticast | mac-notification** [**change**] [**move**] [**threshold**] | **mpls | msdp | ospf** [**cisco-specific | errors | lsa | rate-limit | retransmit | state-change**] | **pim [invalid-pim-message | neighbor-change | rp-mapping-change] | port-security** [**trap-rate** *value*] | **rtr | snmp** [**authentication | coldstart | linkdown | linkup | warmstart**] | **storm-control trap-rate** *value* | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog | transceiver all | tty | vlan-membership | vlancreate | vlandelete**]

Syntax Description

alarms *severity*	(Optional) Enables SNMP alarms traps. For severity, enter number **1** to **4** or enter one of these keywords: • **critical**—Service-affecting condition, severity 1. • **major**—Immediate action needed, severity 2. • **minor**—Minor warning conditions, severity 3. • **informational**—Informational notifications, severity 4.
auth-framework	Enables SNMP CISCO-AUTH-FRAMEWORK-MIB traps
bgp	(Optional) Enables Border Gateway Protocol (BGP) state-change traps. **Note** This keyword is supported only when the metro IP access image is running on the switch.
bridge [**newroot**] [**topologychange**]	(Optional) Generates Spanning Tree Protocol (STP) bridge MIB traps. The keywords have these meanings: • **newroot**—(Optional) Enables SNMP STP bridge MIB new root traps. • **topologychange**—(Optional) Enables SNMP STP bridge MIB topology change traps.

cef *type*	(Optional) Displays Cisco Express Forwarding (CEF) traps. You can optionally enter one of these keywords: • **inconsistency**—Enables SNMP CEF inconsistency traps. • **peer-fib-state-change**—Enables SNMP CEF peer FIB state-change traps. • **peer-state-change**—Enables SNMP CEF peer state-change traps. • **resource-failure**—Enables SNMP CEF resource-failure traps.
config	(Optional) Enables SNMP configuration traps.
copy-config	(Optional) Enable SNMP copy-configuration traps.
cpu threshold	(Optional) Allows CPU-related traps.
entity	(Optional) Enables SNMP entity traps.
envmon [**fan** | **shutdown** | **status** | **supply** | **temperature**]	Optional) Enables SNMP environmental traps. The keywords have these meanings: • **fan**—(Optional) Enables fan traps. • **shutdown**—(Optional) Enables environmental monitor shutdown traps. • **status**—(Optional) Enables SNMP environmental status-change traps. • **supply**—(Optional) Enables environmental monitor power-supply traps. • **temperature**—(Optional) Enables environmental monitor temperature traps.
ether oam	(Optional) Enables Ethernet OAM traps.
ethernet	(Optional) Enables SNMP Ethernet traps.
flash	(Optional) Enables SNMP flash notifications.
hsrp	(Optional) Enables Hot Standby Router Protocol (HSRP) traps.
ipmulticast	(Optional) Enables IP multicast routing traps.
mac-notification	(Optional) Enables MAC address notification traps.
change	(Optional) Enables MAC address change notification traps.
move	(Optional) Enables MAC address move notification traps.
mpls	(Optional) Enables multiprotocol label switching (MPLS) traps.
threshold	(Optional) Enables MAC address table threshold traps.
msdp	(Optional) Enables Multicast Source Discovery Protocol (MSDP) traps.
ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** | **retransmit** | **state-change**]	(Optional) Enables Open Shortest Path First (OSPF) traps. The keywords have these meanings: • **cisco-specific**—(Optional) Enables Cisco-specific traps. • **errors**—(Optional) Enables error traps. • **lsa**—(Optional) Enables link-state advertisement (LSA) traps. • **rate-limit**—(Optional) Enables rate-limit traps. • **retransmit**—(Optional) Enables packet-retransmit traps. • **state-change**—(Optional) Enables state-change traps.

pim [**invalid-pim-message** | **neighbor-change** | **rp-mapping-change**]	(Optional) Enables Protocol-Independent Multicast (PIM) traps. The keywords have these meanings: • **invalid-pim-message**—(Optional) Enables invalid PIM message traps. • **neighbor-change**—(Optional) Enables PIM neighbor-change traps. • **rp-mapping-change**—(Optional) Enables rendezvous point (RP)-mapping change traps.
rtr	(Optional) Enables SNMP Response Time Reporter traps.
snmp [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]	(Optional) Enables SNMP traps. The keywords have these meanings: • **authentication**—(Optional) Enables authentication trap. • **coldstart**—(Optional) Enables cold-start trap. • **linkdown**—(Optional) Enables linkdown trap. • **linkup**—(Optional) Enables linkup trap. • **warmstart**—(Optional) Enables warm-start trap.
storm-control trap-rate *value*	(Optional) Enables storm-control traps. Use the **trap-rat**e keyword to set the maximum number of storm-control traps sent per minute. The range is from 0 to 1000; the default is 0 (no limit is imposed; a trap is sent at every storm-control occurrence).
stpx [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**]	(Optional) Enables SNMP STPX MIB traps. The keywords have these meanings: • **inconsistency**—(Optional) Enables SNMP STPX MIB inconsistency update traps. • **root-inconsistency**—(Optional) Enables SNMP STPX MIB root inconsistency update traps. • **loop-inconsistency**—(Optional) Enables SNMP STPX MIB loop inconsistency update traps.
syslog	(Optional) Enables SNMP syslog traps.
transceiver all	(Optional) Enables SNMP traps for all supported Digital Optical Monitoring (DoM)-capable transceivers installed on the switch.
tty	(Optional) Sends TCP connection traps. This is enabled by default.
vlan-membership	(Optional) Enables SNMP VLAN membership traps.
vlancreate	(Optional) Enables SNMP VLAN-created traps.
vlandelete	(Optional) Enables SNMP VLAN-deleted traps.

Note Though visible in the command-line help strings, the **dot1x**, **energywise**, **event-manager**, **fru-ctrl insertion** and **removal**, and **vtp** keywords are not supported. The **snmp-server enable informs** global configuration command is not supported. To enable the sending of SNMP inform notifications, use the **snmp-server enable traps** global configuration command combined with the **snmp-server host** *host-addr* **informs** global configuration command.

Defaults

The sending of SNMP traps is disabled.

Command Modes Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

When supported, use the **snmp-server enable traps** command to enable sending of traps or informs.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

SNMP transceiver traps apply to SFPs that support DoM-capable transceivers installed on the switch. The sensor values are polled every 10 minutes, which is how often the user sees traps or alarms.

You can verify your setting by entering the **show running-config** privileged EXEC command.

Examples This example shows how to send MPLS traps to the NMS:

```
Switch(config)# snmp-server enable traps mpls
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
snmp-server host	Specifies the host that receives SNMP traps.

snmp-server host

To specify the recipient (host) of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host, use the **no** form of this command.

snmp-server host *host-addr* [**informs | traps**] [**version** {**1 | 2c | 3** {**auth | noauth| priv**}] [**vrf** *vrf-instance*] {*community-string* [*notification-type*]}

no snmp-server host *host-addr* [**informs | traps**] [**version** {**1 | 2c | 3** {**auth | noauth | priv**}] [**vrf** *vrf-instance*] *community-string*

Syntax Description

host-addr	Name or Internet address of the host (the targeted recipient).
udp-port *port*	(Optional) Configures the User Datagram Protocol (UDP) port number of the host to receive the traps. The range is from 0 to 65535.
informs | traps	(Optional) Sends SNMP traps or informs to this host.
version 1 | 2c | 3	(Optional) Version of the SNMP used to send the traps. These keywords are supported: **1**—SNMPv1. This option is not available with informs. **2c**—SNMPv2C. **3**—SNMPv3. These optional keywords can follow the Version 3 keyword: • **auth** (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. • **noauth** (Default). The noAuthNoPriv security level. This is the default if the [**auth | noauth | priv**] keyword choice is not specified. • **priv** (Optional). Enables Data Encryption Standard (DES) packet encryption (also called *privacy*). **Note** The **priv** keyword is available only when the cryptographic (encrypted) software image is installed.
vrf *vrf-instance*	(Optional) Virtual private network (VPN) routing instance and name for this host.
community-string	Password-like community string sent with the notification operation. Though you can set this string by using the **snmp-server host** command, we recommend that you define this string by using the **snmp-server community** global configuration command before using the **snmp-server host** command. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

notification-type (Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent.

- **alarms**—Sends SNMP alarms traps.
- **auth-framework**—Sends NMP CISCO-AUTH-FRAMEWORK-MIB traps.
- **bgp**—Sends Border Gateway Protocol (BGP) state change traps. This keyword is valid only when the metro IP access image is installed on the switch.
- **bridge**—Sends SNMP Spanning Tree Protocol (STP) bridge MIB traps.
- **cef**—Sends cef traps.
- **config**—Sends SNMP configuration traps.
- **copy-config**—Sends SNMP copy configuration traps.
- **config-ctid** —Sends SNMP config-ctid traps.
- **cpu threshold**—Allows CPU-related traps.
- **eigrp**—Sends SNMP EIGRP traps
- **entity**— Sends SNMP entity traps.
- **envmon**—Sends environmental monitor traps.
- **ethernet-cfm**—Sends SNMP Ethernet CFM traps.
- **flash**—Sends SNMP FLASH notifications.
- **hsrp—**Sends SNMP Hot Standby Router Protocol (HSRP) traps.
- **ipmulticast—**Sends SNMP IP multicast routing traps.
- **isis**—Sends IS-IS traps.
- **license**—Sends license traps.
- **mac-notification—**Sends SNMP MAC notification traps.
- **mpls-fast-reroute**—Sends SNMP MPLS traffic engineering fast reroute traps.
- **mpls-ldp**—Sends SNMP MPLS label distribution protocol traps.
- **mpls-traffic-eng**—Sends SNMP MPLS traffic engineering traps.
- **mpls-vpn**—Sends SNMP MPLS Virtual Private Network traps.
- **msdp—**Sends SNMP Multicast Source Discovery Protocol (MSDP) traps.
- **ospf—**Sends Open Shortest Path First (OSPF) traps.
- **pim—**Sends SNMP Protocol-Independent Multicast (PIM) traps.
- **rtr—**Sends SNMP Response Time Reporter traps.
- **snmp—**Sends SNMP-type traps.
- **stpx—**Sends SNMP STP extended MIB traps.
- **syslog—**Sends SNMP syslog traps.
- **tty—**Sends TCP connection traps.
- **vlan-membership—** Sends SNMP VLAN membership traps.
- **vlancreate—**Sends SNMP VLAN-created traps.
- **vlandelete—**Sends SNMP VLAN-deleted traps.

Note Though visible in the command-line help strings, the **energywise**, **event manager**, **fru-ctrl**, and **vtp** keywords are not supported.

Defaults

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is Version 1.

If Version 3 is selected and no authentication keyword is entered, the default is the **noauth** (noAuthNoPriv) security level.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destinations.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Traps are also sent only once, but an inform might be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. To enable multiple hosts, you must enter a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

If a local user is not associated with a remote host, the switch does not send informs for the **auth** (authNoPriv) and the **priv** (authPriv) authentication levels.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command replaces the first.

The **snmp-server host** command is used with the **snmp-server enable traps** global configuration command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable traps** command and

the **snmp-server host** command for that host must be enabled. Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled. Other notification types are enabled by a different command.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

You can verify your settings by entering the **show running-config** privileged EXEC command.

Examples

This example shows how to configure a unique SNMP community string named *comaccess* for traps and prevent SNMP polling access with this string through access-list 10:

```
Switch(config)# snmp-server community comaccess ro 10
Switch(config)# snmp-server host 172.20.2.160 comaccess
Switch(config)# access-list 10 deny any
```

This example shows how to send the SNMP traps to the host specified by the name *myhost.cisco.com*. The community string is defined as *comaccess*:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com comaccess snmp
```

This example shows how to enable the switch to send all traps to the host *myhost.cisco.com* by using the community string *public*:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
snmp-server enable traps	Enables SNMP notification for various trap types or inform requests.

snmp trap mac-notification change

To enable the Simple Network Management Protocol (SNMP) MAC address notification trap on a specific Layer 2 interface, use the **snmp trap mac-notification change** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

snmp trap mac-notification change {**added | removed**}

no snmp trap mac-notification change {**added | removed**}

Syntax Description

added	Enables the MAC notification trap whenever a MAC address is added on this interface.
removed	Enables the MAC notification trap whenever a MAC address is removed from this interface.

Defaults

By default, the traps for both address addition and address removal are disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Even though you enable the notification trap for a specific interface by using the **snmp trap mac-notification** command, the trap is generated only when you enable the **snmp-server enable traps mac-notification** and the **mac address-table notification** global configuration commands.

You can verify your settings by entering the **show mac address-table notification change interface** privileged EXEC command.

Examples

This example shows how to enable the MAC notification trap when a MAC address is added to a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# snmp trap mac-notification change added
```

Related Commands

Command	Description
clear mac address-table notification	Clears the MAC address notification global counters.
mac address-table notification	Enables the MAC address notification feature.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or on the specified interface when the **interface** keyword is appended.
snmp-server enable traps	Sends the SNMP MAC notification traps when the **mac-notification** keyword is appended.

spanning-tree bpdufilter

To prevent an interface from sending or receiving bridge protocol data units (BPDUs), use the **spanning-tree bpdufilter** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree bpdufilter {**disable** | **enable**}

no spanning-tree bpdufilter

Syntax Description

disable	Disables BPDU filtering on the specified STP port.
enable	Enables BPDU filtering on the specified STP port.

Defaults

BPDU filtering is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can enable the BPDU filtering feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

Caution Enabling BPDU filtering on an STP port is the same as disabling spanning tree on it and can result in spanning-tree loops.

You can globally enable BPDU filtering on all Port Fast-enabled STP ports by using the **spanning-tree portfast bpdufilter default** global configuration command.

You can use the **spanning-tree bpdufilter** interface configuration command on an STP port to override the setting of the **spanning-tree portfast bpdufilter default** global configuration command.

You can verify your setting by entering the **show running-config** privileged EXEC command.

Examples

This example shows how to enable the BPDU filtering feature on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpdufilter enable
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled STP ports or enables the Port Fast feature on all nontrunking STP ports.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an STP port and all its associated VLANs.

spanning-tree bpduguard

To put an interface in the error-disabled state when it receives a bridge protocol data unit (BPDU), use the **spanning-tree bpduguard** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree bpduguard {**disable** | **enable**}

no spanning-tree bpduguard

Syntax Description

disable	Disables BPDU guard on the specified STP port.
enable	Enables BPDU guard on the specified STP port.

Defaults

BPDU guard is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The BPDU guard feature provides a secure response to invalid configurations because you must manually put the STP port back in service. Use the BPDU guard feature in a service-provider network to prevent an interface from being included in the spanning-tree topology.

You can enable the BPDU guard feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), the rapid-PVST+, or the multiple spanning-tree (MST) mode.

You can globally enable BPDU guard on all Port Fast-enabled STP ports by using the **spanning-tree portfast bpduguard default** global configuration command.

You can use the **spanning-tree bpduguard** interface configuration command on an STP port to override the setting of the **spanning-tree portfast bpduguard default** global configuration command.

You can verify your setting by entering the **show running-config** privileged EXEC command.

Examples

This example shows how to enable the BPDU guard feature on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpduguard enable
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled STP ports or enables the Port Fast feature on all nontrunking STP ports.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an STP port and all its associated VLANs.

spanning-tree cost

To set the path cost for spanning-tree calculations. use the **spanning-tree cost** command in interface configuration mode. If a loop occurs, spanning tree considers the path cost when selecting an interface to place in the forwarding state. To return to the default setting, use the **no** form of this command.

spanning-tree [**vlan** *vlan-id*] **cost** *cost*

no spanning-tree [**vlan** *vlan-id*] **cost**

Syntax Description

vlan *vlan-id*	(Optional) VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
cost	Path cost. The range is 1 to 200000000, with higher values meaning higher costs.

Defaults

The default path cost is computed from the STP interface bandwidth setting. These are the IEEE default path cost values:

- 1000 Mbps—1
- 100 Mbps—10
- 10 Mbps—100

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When you configure the cost, higher values represent higher costs.

If you configure an STP port with both the **spanning-tree vlan** *vlan-id* **cost** *cost* command and the **spanning-tree cost** *cost* command, the **spanning-tree vlan** *vlan-id* **cost** *cost* command takes effect.

You can verify your settings by entering the **show spanning-tree interface** *interface-id* privileged EXEC command.

Examples

This example shows how to set the path cost to 250 on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree cost 250
```

This example shows how to set a path cost to 300 for VLANs 10, 12 to 15, and 20:

```
Switch(config-if)# spanning-tree vlan 10,12-15,20 cost 300
```

Related Commands

Command	Description
show spanning-tree interface *interface-id*	Displays spanning-tree information for the specified interface.
spanning-tree port-priority	Configures an STP port priority.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree etherchannel guard misconfig

To display an error message when the switch detects an EtherChannel misconfiguration, use the **spanning-tree etherchannel guard misconfig** command in global configuration mode. To disable the feature, use the **no** form of this command.

spanning-tree etherchannel guard misconfig

no spanning-tree etherchannel guard misconfig

Syntax Description

This command has no arguments or keywords.

Defaults

EtherChannel guard is enabled on the switch.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When the switch detects an EtherChannel misconfiguration, this error message appears:

```
PM-4-ERR_DISABLE: Channel-misconfig error detected on [chars], putting [chars] in
err-disable state.
```

To show switch ports that are in the misconfigured EtherChannel, use the **show interfaces status err-disabled** privileged EXEC command. To verify the EtherChannel configuration on a remote device, use the **show etherchannel summary** privileged EXEC command on the remote device.

When a port is in the error-disabled state because of an EtherChannel misconfiguration, you can bring it out of this state by entering the **errdisable recovery cause channel-misconfig** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

You can verify your settings by entering the **show spanning-tree summary** privileged EXEC command.

Examples

This example shows how to enable the EtherChannel guard misconfiguration feature:

```
Switch(config)# spanning-tree etherchannel guard misconfig
```

Related Commands

Command	Description
errdisable recovery cause channel-misconfig	Enables the timer to recover from the EtherChannel misconfiguration error-disable state.
show etherchannel summary	Displays EtherChannel information for a channel as a one-line summary per channel-group.
show interfaces status err-disabled	Displays the interfaces in the error-disabled state.

spanning-tree extend system-id

To enable the extended system ID feature, use the **spanning-tree extend system-id** global configuration command.

spanning-tree extend system-id

Note Though visible in the command-line help strings, the **no** version of this command is not supported. You cannot disable the extended system ID feature.

Syntax Description

This command has no arguments or keywords.

Defaults

The extended system ID is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The switch supports the IEEE 802.1t spanning-tree extensions. Some of the bits previously used for the switch priority are now used for the extended system ID (VLAN identifier for the per-VLAN spanning-tree plus [PVST+] and rapid PVST+ or as an instance identifier for the multiple spanning tree [MST]).

The spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN or multiple spanning-tree instance.

Support for the extended system ID affects how you manually configure the root switch, the secondary root switch, and the switch priority of a VLAN. For more information, see the "spanning-tree mst root" and the "spanning-tree vlan" sections.

If your network consists of switches that do not support the extended system ID and switches that do support it, it is unlikely that the switch with the extended system ID support will become the root switch. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected switches.

Related Commands

Command	Description
show spanning-tree summary	Displays a summary of spanning-tree interface states.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree guard

To enable root guard or loop guard on all the VLANs associated with the selected port, use the **spanning-tree guard** command in interface configuration mode. Root guard restricts which interface is allowed to be the spanning-tree root port or the path-to-the root for the switch. Loop guard prevents alternate or root ports from becoming designated ports when a failure creates a unidirectional link. To return to the default setting, use the **no** form of this command.

spanning-tree guard {**loop** | **none** | **root**}

no spanning-tree guard

Syntax Description

loop	Enabled loop guard.
none	Disabled root guard or loop guard.
root	Enabled root guard.

Defaults

Root guard is disabled.

Loop guard is configured according to the **spanning-tree loopguard default** global configuration command (globally disabled).

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can enable root guard or loop guard when the switch is operating in the per-VLAN spanning-tree plus (PVST+), the rapid-PVST+, or the multiple spanning-tree (MST) mode.

When root guard is enabled, if spanning-tree calculations cause an interface to be selected as the root port, the interface transitions to the root-inconsistent (blocked) state to prevent the customer's switch from becoming the root switch or being in the path to the root. The root port provides the best path from the switch to the root switch.

When the **no spanning-tree guard** or the **no spanning-tree guard none** command is entered, root guard is disabled for all VLANs on the selected NNI. If this interface is in the root-inconsistent (blocked) state, it automatically transitions to the listening state.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary interfaces if the interface is blocked by loop guard in all MST instances. On a boundary interface, loop guard blocks the interface in all MST instances.

To disable root guard or loop guard, use the **spanning-tree guard none** interface configuration command on an STP interface. You cannot enable both root guard and loop guard at the same time.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command on an STP interface.

You can verify your settings by entering the **show running-config** privileged EXEC command.

Examples

This example shows how to enable root guard on all the VLANs associated with the specified port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard root
```

This example shows how to enable loop guard on all the VLANs associated with the specified port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard loop
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree loopguard default	Prevents alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link.
spanning-tree mst cost	Configures the path cost for MST calculations.
spanning-tree mst port-priority	Configures an STP MST port priority.
spanning-tree mst root	Configures the MST root switch priority and timers based on the network diameter.
spanning-tree port-priority	Configures an STP port priority.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree link-type

To override the default link-type setting, which is determined by the duplex mode of the Spanning Tree Protocol (STP) port, and to enable rapid spanning-tree transitions to the forwarding state, use the **spanning-tree link-type** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree link-type {**point-to-point** | **shared**}

no spanning-tree link-type

Syntax Description

point-to-point	Specifies that the link type of an STP port is point-to-point.
shared	Specifies that the link type of an STP port is shared.

Defaults

The switch derives the link type of an interface from the duplex mode. A full-duplex interface is considered a point-to-point link, and a half-duplex interface is considered a shared link.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can override the default setting of the link type by using the **spanning-tree link-type** command. For example, a half-duplex link can be physically connected point-to-point to a single interface on a remote switch running the Multiple Spanning Tree Protocol (MSTP) or the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol and be enabled for rapid transitions.

You can verify your setting by entering the **show spanning-tree mst interface** *interface-id* or the show **spanning-tree interface** *interface-id* privileged EXEC command.

Examples

This example shows how to specify the link type as shared (regardless of the duplex setting) and to prevent rapid transitions to the forwarding state:

```
Switch(config-if)# spanning-tree link-type shared
```

Related Commands

Command	Description
clear spanning-tree counters	Restarts the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface.
show spanning-tree interface *interface-id*	Displays spanning-tree state information for the specified interface.
show spanning-tree mst interface *interface-id*	Displays MST information for the specified interface.

spanning-tree loopguard default

To enable loopguard by default on all interfaces with STP enabled, use the **spanning-tree loopguard default** command in global configuration mode. Enabling loopguard prevents alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. To return to the default setting, use the **no** form of this command.

spanning-tree loopguard default

no spanning-tree loopguard default

Syntax Description

This command has no arguments or keywords.

Defaults

Loop guard is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.252)EY	This command was introduced.

Usage Guidelines

You can enable the loop guard feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary interfaces if the interface is blocked by loop guard in all MST instances. On a boundary interface, loop guard blocks the interface in all MST instances.

Loop guard operates only on STP ports that the spanning tree identifies as point-to-point.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command.

You can verify your settings by entering the **show running-config** privileged EXEC command.

Examples

This example shows how to globally enable loop guard:

```
Switch(config)# spanning-tree loopguard default
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree guard loop	Enables the loop guard feature on all the VLANs associated with the specified STP port.

spanning-tree mode

To enable per-VLAN spanning-tree plus (PVST+), rapid PVST+, or multiple spanning tree (MST), use the **spanning-tree mode** command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree mode {**mst** | **pvst** | **rapid-pvst**}

no spanning-tree mode

Syntax Description

mst	Enables MST and Rapid Spanning Tree Protocol (RSTP) (based on IEEE 802.1s and IEEE 802.1w).
pvst	Enables PVST+ (based on IEEE 802.1D).
rapid-pvst	Enables rapid PVST+ (based on IEEE 802.1w).

Defaults

The default mode is rapid PVST+.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The switch supports PVST+, rapid PVST+, and MSTP, but only one version can be active at any time: All VLANs run PVST+, all VLANs run rapid PVST+, or all VLANs run MSTP.

When you enable the MST mode, RSTP is automatically enabled.

Caution Changing spanning-tree modes can disrupt traffic because all spanning-tree instances are stopped for the previous mode and restarted in the new mode.

You can verify your setting by entering the **show running-config** privileged EXEC command.

Examples

This example shows to enable MST and RSTP on the switch:

```
Switch(config)# spanning-tree mode mst
```

This example shows to enable PVST+ on the switch:

```
Switch(config)# spanning-tree mode pvst
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.

spanning-tree mst configuration

To enter multiple spanning-tree (MST) configuration mode through which you configure the MST region, use the **spanning-tree mst configuration** command in global configuration mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst configuration

no spanning-tree mst configuration

Syntax Description

This command has no arguments or keywords.

Defaults

The default mapping is that all VLANs are mapped to the common and internal spanning-tree (CIST) instance (instance 0).

The default name is an empty string.

The revision number is 0.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **spanning-tree mst configuration** command enables the MST configuration mode. These configuration commands are available:

- **abort**: exits the MST region configuration mode without applying configuration changes.
- **exit**: exits the MST region configuration mode and applies all configuration changes.
- **instance** *instance-id* **vlan** *vlan-range*: maps VLANs to an MST instance. The range for the *instance-id* is 0 to 4094. The range for *vlan-range* is 1 to 4094. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.
- **name** *name*: sets the configuration name. The *name* string has a maximum length of 32 characters and is case sensitive.
- **no**: negates the **instance**, **name**, and **revision** commands or sets them to their defaults.
- **private-vlan**: Although visible in the command-line help strings, this command is not supported.
- **revision** *version*: sets the configuration revision number. The range is 0 to 65535.
- **show** [**current** | **pending**]: displays the current or pending MST region configuration.

In MST mode, the switch supports up to 16 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.

When you map VLANs to an MST instance, the mapping is incremental, and VLANs specified in the command are added to or removed from the VLANs that were previously mapped. To specify a range, use a hyphen; for example, **instance 1 vlan 1-63** maps VLANs 1 to 63 to MST instance 1. To specify a series, use a comma; for example, **instance 1 vlan 10, 20, 30** maps VLANs 10, 20, and 30 to MST instance 1.

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST by using the **no** form of the command.

For two or more switches to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

You can verify your settings by entering the **show pending** MST configuration command.

Examples

This example shows how to enter MST configuration mode, map VLANs 10 to 20 to MST instance 1, name the region *region1*, set the configuration revision to 1, display the pending configuration, apply the changes, and return to global configuration mode:

```
Switch# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
--------  ---------------------
0         1-9,21-4094
1         10-20
-------------------------------

Switch(config-mst)# exit
Switch(config)#
```

This example shows how to add VLANs 1 to 100 to the ones already mapped (if any) to instance 2, to move VLANs 40 to 60 that were previously mapped to instance 2 to the CIST instance, to add VLAN 10 to instance 10, and to remove all the VLANs mapped to instance 2 and map them to the CIST instance:

```
Switch(config-mst)# instance 2 vlan 1-100
Switch(config-mst)# no instance 2 vlan 40-60
Switch(config-mst)# instance 10 vlan 10
Switch(config-mst)# no instance 2
```

Related Commands

Command	Description
show spanning-tree mst configuration	Displays the MST region configuration.

spanning-tree mst cost

To set the path cost for multiple spanning-tree (MST) calculations, use the **spanning-tree mst cost** command in interface configuration mode. If a loop occurs, spanning tree considers the path cost when selecting an interface to put in the forwarding state. To return to the default setting, use the **no** form of this command.

spanning-tree mst *instance-id* **cost** *cost*

no spanning-tree mst *instance-id* **cost**

Syntax Description

instance-id	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.
cost	Path cost is 1 to 200000000, with higher values meaning higher costs.

Defaults

The default path cost is computed from the interface speed. Faster speeds have smaller costs.

- 10 Gb/s—2000
- 1000 Mb/s—20000
- 100 Mb/s—200000
- 10 Mbp\/s—2000000

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When you configure the cost, higher values represent higher costs.

You can verify your settings by entering the **show spanning-tree mst interface** *interface-id* privileged EXEC command.

Examples

This example shows how to set a path cost of 250 on a port associated with instances 2 and 4:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 2,4 cost 250
```

Related Commands

Command	Description
show spanning-tree mst interface *interface-id*	Displays MST information for the specified interface.
spanning-tree mst port-priority	Configures an interface priority.
spanning-tree mst priority	Configures the switch priority for the specified spanning-tree instance.

spanning-tree mst forward-time

To set the forward-delay time for all multiple spanning-tree (MST) instances, use the **spanning-tree mst forward-time** command in global configuration mode. The forwarding time specifies how long each of the listening and learning states last before the interface begins forwarding. To return to the default setting, use the **no** form of this command.

spanning-tree mst forward-time *seconds*

no spanning-tree mst forward-time

Syntax Description

seconds	Length of the listening and learning states. The range is 4 to 30 seconds.

Defaults

The default is 15 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Changing the **spanning-tree mst forward-time** command affects all spanning-tree instances.

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Examples

This example shows how to set the spanning-tree forwarding time to 18 seconds for all MST instances:

```
Switch(config)# spanning-tree mst forward-time 18
```

Related Commands

Command	Description
show spanning-tree mst	Displays MST information.
spanning-tree mst hello-time	Sets the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst hello-time

To set the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages, use the **spanning-tree mst hello-time** command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree mst hello-time *seconds*

no spanning-tree mst hello-time

Syntax Description

seconds	Interval between hello BPDUs sent by root switch configuration messages. The range is 1 to 10 seconds.

Defaults

The default is 2 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

After you set the **spanning-tree mst max-age** *seconds* global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

Changing the **spanning-tree mst hello-time** command affects all spanning-tree instances.

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Examples

This example shows how to set the spanning-tree hello time to 3 seconds for all multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst hello-time 3
```

Related Commands

Command	Description
show spanning-tree mst	Displays MST information.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst max-age

To set the interval between messages that the spanning tree receives from the root switch, use the **spanning-tree mst max-age** command in global configuration mode. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputes the spanning-tree topology. To return to the default setting, use the **no** form of this command.

spanning-tree mst max-age *seconds*

no spanning-tree mst max-age

Syntax Description

seconds	Interval between messages the spanning tree receives from the root switch. The range is 6 to 40 seconds.

Defaults

The default is 20 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

After you set the **spanning-tree mst max-age** *seconds* global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

Changing the **spanning-tree mst max-age** command affects all spanning-tree instances.

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Examples

This example shows how to set the spanning-tree max-age to 30 seconds for all multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst max-age 30
```

Related Commands

Command	Description
show spanning-tree mst	Displays MST information.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree mst max-hops

To set the number of hops in a region before the bridge protocol data unit (BPDU) is discarded and the information held for an interface is aged, use the **spanning-tree mst max-hops** command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree mst max-hops *hop-count*

no spanning-tree mst max-hops

Syntax Description

hop-count	Number of hops in a region before the BPDU is discarded. The range is 1 to 255 hops.

Defaults

The default is 20 hops.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The root switch of the instance always sends a BPDU (or M-record) with a cost of 0 and the hop count set to the maximum value. When a switch receives this BPDU, it decrements the received remaining hop count by one and propagates the decremented count as the remaining hop count in the generated M-records. A switch discards the BPDU and ages the information held for the interface when the count reaches 0.

Changing the **spanning-tree mst max-hops** command affects all spanning-tree instances.

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

Examples

This example shows how to set the spanning-tree max-hops to 10 for all multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst max-hops 10
```

Related Commands

Command	Description
show spanning-tree mst	Displays MST information.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.

spanning-tree mst port-priority

To configure an interface priority, use the **spanning-tree mst port-priority** command in interface configuration mode. If a loop occurs, the Multiple Spanning Tree Protocol (MSTP) can find the interface to put in the forwarding state. To return to the default setting, use the **no** form of this command.

spanning-tree mst *instance-id* **port-priority** *priority*

no spanning-tree mst *instance-id* **port-priority**

Syntax Description

instance-id	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.
priority	The range is 0 to 240 in increments of 16. Valid priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority.

Defaults

The default is 128.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can assign higher priority values (lower numerical values) to STP port that you want selected first and lower priority values (higher numerical values) that you want selected last. If all STP ports have the same priority value, the multiple spanning tree (MST) puts the interface with the lowest interface number in the forwarding state and blocks other interfaces.

You can verify your settings by entering the **show spanning-tree mst interface** *interface-id* privileged EXEC command.

Examples

This example shows how to increase the likelihood that the interface associated with spanning-tree instances 20 and 22 is placed into the forwarding state if a loop occurs:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 20,22 port-priority 0
```

Related Commands

Command	Description
show spanning-tree mst interface *interface-id*	Displays MST information for the specified interface.
spanning-tree mst cost	Sets the path cost for MST calculations.
spanning-tree mst priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree mst pre-standard

To configure a port to send only prestandard bridge protocol data units (BPDUs), use the **spanning-tree mst pre-standard** command in interface configuration command. To return to the default setting, use the **no** form of this command.

spanning-tree mst pre-standard

no spanning-tree mst pre-standard

Syntax Description

This command has no arguments or keywords.

Command Default

The default state is automatic detection of prestandard neighbors.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The port can accept both prestandard and standard BPDUs. If the neighbor types are mismatched, only the common and internal spanning tree (CIST) runs on this interface.

Note If a switch port is connected to a switch running prestandard Cisco IOS software, you *must* use the **spanning-tree mst pre-standard** interface configuration command on the port. If you do not configure the port to send only prestandard BPDUs, the Multiple STP (MSTP) performance might diminish.

When the port is configured to automatically detect prestandard neighbors, the *prestandard* flag always appears in the **show spanning-tree mst** commands.

You can verify your settings by entering the **show spanning-tree mst** privileged EXEC command.

Examples

This example shows how to configure a port to send only prestandard BPDUs:

```
Switch(config-if)# spanning-tree mst pre-standard
```

Related Commands

Command	Description
show spanning-tree mst *instance-id*	Displays multiple spanning-tree (MST) information, including the *prestandard* flag, for the specified interface.

spanning-tree mst priority

To set the switch priority for the specified spanning-tree instance, use the **spanning-tree mst priority** command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree mst *instance-id* **priority** *priority*

no spanning-tree mst *instance-id* **priority**

Syntax Description

instance-id	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.
priority	Sets the switch priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. The range is 0 to 61440 in increments of 4096. Valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

Defaults

The default is 32768.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to set the spanning-tree priority to 8192 for multiple spanning-tree instances (MST) 20 to 21:

```
Switch(config)# spanning-tree mst 20-21 priority 8192
```

Related Commands

Command	Description
show spanning-tree mst *instance-id*	Displays MST information for the specified interface.
spanning-tree mst cost	Sets the path cost for MST calculations.
spanning-tree mst port-priority	Configures an interface priority.

spanning-tree mst root

Use the **spanning-tree mst root** global configuration command to configure the multiple spanning-tree (MST) root switch priority and timers based on the network diameter. Use the **no** form of this command to return to the default settings.

spanning-tree mst *instance-id* **root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]

no spanning-tree mst *instance-id* **root**

Syntax Description

instance-id	Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094.
root primary	Forces this switch to be the root switch.
root secondary	Sets this switch to be the root switch should the primary root switch fail.
diameter *net-diameter*	(Optional) Sets the maximum number of switches between any two end stations. The range is 2 to 7. This keyword is available only for MST instance 0.
hello-time *seconds*	(Optional) Sets the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds. This keyword is available only for MST instance 0.

Defaults

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

The hello time is 2 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use the **spanning-tree mst** *instance-id* **root** command only on backbone switches.

When you enter the **spanning-tree mst** *instance-id* **root** command, the software tries to set a high enough priority to make this switch the root of the spanning-tree instance. Because of the extended system ID support, the switch sets the switch priority for the instance to 24576 if this value will cause this switch to become the root for the specified instance. If any root switch for the specified instance has a switch priority lower than 24576, the switch sets its own priority to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree mst** *instance-id* **root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch fails, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768 and are therefore unlikely to become the root switch).

You can verify your settings by entering the **show spanning-tree mst** *instance-id* privileged EXEC command.

Examples

This example shows how to configure the switch as the root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root secondary diameter 4
```

Related Commands

Command	Description
show spanning-tree mst *instance-id*	Displays MST information for the specified instance.
spanning-tree mst forward-time	Sets the forward-delay time for all MST instances.
spanning-tree mst hello-time	Sets the interval between hello BPDUs sent by root switch configuration messages.
spanning-tree mst max-age	Sets the interval between messages that the spanning tree receives from the root switch.
spanning-tree mst max-hops	Sets the number of hops in a region before the BPDU is discarded.

spanning-tree port-priority

To configure an interface priority, use the **spanning-tree port-priority** command in interface configuration mode. If a loop occurs, spanning tree can find the interface to put in the forwarding state. To return to the default setting, use the **no** form of this command.

spanning-tree [**vlan** *vlan-id*] **port-priority** *priority*

no spanning-tree [**vlan** *vlan-id*] **port-priority**

Syntax Description

vlan *vlan-id*	(Optional) VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
priority	Number from 0 to 240, in increments of 16. Valid values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority.

Defaults

The default is 128.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If the variable *vlan-id* is omitted, the command applies to the spanning-tree instance associated with VLAN 1.

You can set the priority on a VLAN that has no interfaces assigned to it. The setting takes effect when you assign the STP port to the VLAN.

If you configure an STP port with both the **spanning-tree vlan** *vlan-id* **port-priority** *priority* command and the **spanning-tree port-priority** *priority* command, the **spanning-tree vlan** *vlan-id* **port-priority** *priority* command takes effect.

You can verify your settings by entering the **show spanning-tree interface** *interface-id* privileged EXEC command.

Examples

This example shows how to increase the likelihood that a port will be put in the forwarding state if a loop occurs:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

This example shows how to set the port-priority value on VLANs 20 to 25:

```
Switch(config-if)# spanning-tree vlan 20-25 port-priority 0
```

Related Commands

Command	Description
show spanning-tree interface *interface-id*	Displays spanning-tree information for the specified interface.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree vlan priority	Sets the switch priority for the specified spanning-tree instance.

spanning-tree portfast (global configuration)

To globally enable bridge protocol data unit (BPDU) filtering on Port Fast-enabled interfaces, the BPDU guard feature on Port Fast-enabled STP ports, or the Port Fast feature on all nontrunking STP ports., use the **spanning-tree portfast** command in global configuration mode. The BPDU filtering feature prevents the switch STP port from sending or receiving BPDUs. The BPDU guard feature puts Port Fast-enabled STP ports that receive BPDUs in an error-disabled state. To return to the default settings, use the **no** form of this command.

spanning-tree portfast {**bpdufilter default** | **bpduguard default** | **default**}

no spanning-tree portfast {**bpdufilter default** | **bpduguard default** | **default**}

Syntax Description

bpdufilter default	Globally enables BPDU filtering on Port Fast-enabled STP ports, and prevent the switch STP port connected to end stations from sending or receiving BPDUs.
bpduguard default	Globally enables the BPDU guard feature on Port Fast-enabled STP ports, and place the STP ports that receive BPDUs in an error-disabled state.
default	Globally enables the Port Fast feature on all nontrunking STP ports. When the Port Fast feature is enabled, the STP port changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes.

Defaults

The BPDU filtering, the BPDU guard, and the Port Fast features are disabled on all NNIs or ENIs unless they are individually configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can enable these features when the switch is operating in the per-VLAN spanning-tree plus (PVST+), the rapid-PVST+, or the multiple spanning-tree (MST) mode.

Use the **spanning-tree portfast bpdufilter default** global configuration command to globally enable BPDU filtering on STP ports that are Port Fast-enabled. The STP ports still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to switch STP ports do not receive BPDUs. If a BPDU is received on a Port Fast-enabled STP port, the interface loses its Port Fast-operational status and BPDU filtering is disabled.

You can override the **spanning-tree portfast bpdufilter default** global configuration command on an STP port by using the **spanning-tree bdpufilter** interface configuration command.

Caution Enabling BPDU filtering on an STP port is the same as disabling spanning tree on it and can result in spanning-tree loops.

Use the **spanning-tree portfast bpduguard default** global configuration command to globally enable BPDU guard on STP ports that are in a Port Fast-operational state. In a valid configuration, Port Fast-enabled STP ports do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled STP port signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the STP port in the error-disabled state. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the STP port back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

You can override the **spanning-tree portfast bpduguard default** global configuration command by using the **spanning-tree bdpuguard** interface configuration command on an STP port.

Use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking STP ports. Configure Port Fast only on STP ports that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation. A Port Fast-enabled STP port moves directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-delay time.

You can override the **spanning-tree portfast default** global configuration command by using the **spanning-tree portfast** interface configuration command on an STP port. You can use the **no spanning-tree portfast default** global configuration command to disable Port Fast on all STP ports unless they are individually configured with the **spanning-tree portfast** interface configuration command.

You can verify your settings by entering the **show running-config** privileged EXEC command.

Examples

This example shows how to globally enable the BPDU filtering feature:

```
Switch(config)# spanning-tree portfast bpdufilter default
```

This example shows how to globally enable the BPDU guard feature:

```
Switch(config)# spanning-tree portfast bpduguard default
```

This example shows how to globally enable the Port Fast feature on all nontrunking interfaces:

```
Switch(config)# spanning-tree portfast default
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree bpdufilter	Prevents an interface from sending or receiving BPDUs.
spanning-tree bpduguard	Puts an STP port in the error-disabled state when it receives a BPDU.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an STP port in all its associated VLANs.

spanning-tree portfast (interface configuration)

To enable the Port Fast feature on an STP port in all its associated VLANs, use the **spanning-tree portfast** command in interface configuration mode. When the Port Fast feature is enabled, the STP port changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes. To return to the default setting, use the **no** form of this command.

spanning-tree portfast [**disable** | **trunk**]

no spanning-tree portfast

Syntax Description

disable	(Optional) Disables the Port Fast feature on the specified interface.
trunk	(Optional) Enables the Port Fast feature on a trunking interface.

Defaults

The Port Fast feature is disabled on all ports.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use this feature only on STP ports that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation.

To enable Port Fast on trunk ports, you must use the **spanning-tree portfast trunk** interface configuration command. The **spanning-tree portfast** command is not supported on trunk ports.

You can enable this feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), the rapid-PVST+, or the multiple spanning-tree (MST) mode.

This feature affects all VLANs on the STP port.

An interface with the Port Fast feature enabled is moved directly to the spanning-tree forwarding state without the standard forward-time delay.

You can use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking interfaces. However, the **spanning-tree portfast** interface configuration command can override the global setting.

If you configure the **spanning-tree portfast default** global configuration command, you can disable Port Fast on an STP port that is not a trunk interface by using the **spanning-tree portfast disable** interface configuration command.

You can verify your settings by entering the **show running-config** privileged EXEC command.

Examples

This example shows how to enable the Port Fast feature on a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree portfast
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
spanning-tree bpdufilter	Prevents an interface from sending or receiving bridge protocol data units (BPDUs).
spanning-tree bpduguard	Puts an interface in the error-disabled state when it receives a BPDU.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled STP ports or enables the Port Fast feature on all nontrunking STP ports.

spanning-tree vlan

To configure spanning tree on a per-VLAN basis, use the **spanning-tree vlan** command in global configuration mode. To return to the default setting, use the **no** form of this command.

spanning-tree vlan *vlan-id* [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **priority** *priority* | **root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]]

no spanning-tree vlan *vlan-id* [**forward-time** | **hello-time** | **max-age** | **priority** | **root**]

Syntax Description

vlan-id	VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094.
forward-time *seconds*	(Optional) Sets the forward-delay time for the specified spanning-tree instance. The forwarding time specifies how long each of the listening and learning states last before the interface begins forwarding. The range is 4 to 30 seconds.
hello-time *seconds*	(Optional) Sets the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds.
max-age *seconds*	(Optional) Sets the interval between messages the spanning tree receives from the root switch. If a switch does not receive a BPDU message from the root switch within this interval, it recomputes the spanning-tree topology. The range is 6 to 40 seconds.
priority *priority*	(Optional) Sets the switch priority for the specified spanning-tree instance. This setting affects the likelihood that this switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch. The range is 0 to 61440 in increments of 4096. Valid priority values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.
root primary	(Optional) Forces this switch to be the root switch.
root secondary	(Optional) Sets this switch to be the root switch should the primary root switch fail.
diameter *net-diameter*	(Optional) Sets the maximum number of switches between any two end stations. The range is 2 to 7.

Defaults

Spanning tree is enabled on all VLANs.

The forward-delay time is 15 seconds.

The hello time is 2 seconds.

The max-age is 20 seconds.

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

Command Modes Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines Disabling the STP causes the VLAN to stop participating in the spanning-tree topology. STP ports that are administratively down remain down. Received BPDUs are forwarded like other multicast frames. The VLAN does not detect and prevent loops when STP is disabled.

You can disable the STP on a VLAN that is not currently active and verify the change by using the **show running-config** or the **show spanning-tree vlan** *vlan-id* privileged EXEC command. The setting takes effect when the VLAN is activated.

When disabling or re-enabling the STP, you can specify a range of VLANs that you want to disable or enable.

When a VLAN is disabled and then enabled, all assigned VLANs continue to be its members. However, all spanning-tree bridge parameters are returned to their previous settings (the last setting before the VLAN was disabled).

You can enable spanning-tree options on a VLAN that has no STP ports assigned to it. The setting takes effect when you assign interfaces to it.

When setting the **max-age** *seconds,* if a switch does not receive BPDUs from the root switch within the specified interval, it recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

The **spanning-tree vlan** *vlan-id* **root** command should be used only on backbone switches.

When you enter the **spanning-tree vlan** *vlan-id* **root** command, the software checks the switch priority of the current root switch for each VLAN. Because of the extended system ID support, the switch sets the switch priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN. If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree vlan** *vlan-id* **root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch should fail, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768, and therefore, are unlikely to become the root switch).

You can verify your settings by entering the **show spanning-tree vlan** *vlan-id* privileged EXEC command.

Examples This example shows how to disable the STP on VLAN 5:

```
Switch(config)# no spanning-tree vlan 5
```

You can verify your setting by entering the **show spanning-tree** privileged EXEC command. In this instance, VLAN 5 does not appear in the list.

This example shows how to set the spanning-tree forwarding time to 18 seconds for VLANs 20 and 25:

```
Switch(config)# spanning-tree vlan 20,25 forward-time 18
```

This example shows how to set the spanning-tree hello-delay time to 3 seconds for VLANs 20 to 24:

```
Switch(config)# spanning-tree vlan 20-24 hello-time 3
```

This example shows how to set spanning-tree max-age to 30 seconds for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 max-age 30
```

This example shows how to reset the **max-age** parameter to the default value for spanning-tree instance 100 and 105 to 108:

```
Switch(config)# no spanning-tree vlan 100, 105-108 max-age
```

This example shows how to set the spanning-tree priority to 8192 for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 priority 8192
```

This example shows how to configure the switch as the root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root secondary diameter 4
```

Related Commands

Command	Description
show spanning-tree vlan	Displays spanning-tree information.
spanning-tree cost	Sets the path cost for spanning-tree calculations.
spanning-tree guard	Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface.
spanning-tree port-priority	Sets an interface priority.
spanning-tree portfast (global configuration)	Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled STP ports or enables the Port Fast feature on all nontrunking STP ports.
spanning-tree portfast (interface configuration)	Enables the Port Fast feature on an STP port in all its associated VLANs.

speed

To specify the speed of a 10/100/1000 Mbps port, use the **speed** interface configuration command. To return the port to its default value, use the **no** or **default** form of this command.

speed {**10** | **100** | **1000** | **auto** [**10** | **100** | **1000**] | **nonegotiate**}

no speed

Note You cannot configure the speed on small form-factor pluggable (SFP) module ports or on 10 Gigabit Ethernet ports, but you can configure the speed to not negotiate (**nonegotiate**) if they are connected to a device that does not support autonegotiation. See "Usage Guidelines" for exceptions when a 1000BASE-T SFP module is in the SFP module slot.

Syntax Description

10	Port runs at 10 Mbps.
100	Port runs at 100 Mbps.
1000	Port runs at 1000 Mbps. This option is valid and visible only on 10/100/1000 Mbps-ports.
auto	Port automatically detects the speed it should run at based on the port at the other end of the link. If you use the **10**, **100**, or **1000** keywords with the **auto** keyword, the port only autonegotiates at the specified speeds.
nonegotiate	Autonegotiation is disabled, and the port runs at 1000 Mbps. (The 1000BASE-T SFP does not support the **nonegotiate** keyword.)

Defaults

The default is **auto**.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can configure the Gigabit Ethernet port speed as 10, 100, or 1000 Mbps.

You cannot configure the speed on 10 Gigabit Ethernet ports, but you can configure the speed to not negotiate (**nonegotiate**) if they are connected to a device that does not support autonegotiation.

When a 1000BASE-T SFP module is in the SFP module slot, you can configure the speed as **10**, **100**, **1000**, or auto but not to **nonegotiate**.

Except for the 1000BASE-T SFP modules, if an SFP module port is connected to a device that does not support autonegotiation, you can configure the speed to not negotiate (**nonegotiate**).

If the speed is set to **auto**, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.

If both ends of the line support autonegotiation, we highly recommend the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, do use the **auto** setting on the supported side, but set the duplex and speed on the other side.

Caution Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

Note For guidelines on setting the switch speed and duplex parameters, see the software configuration guide for this release.

You can verify the configuration by entering the **show interfaces** privileged EXEC command.

Examples

This example shows how to set speed on a port to 100 Mbps:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed 100
```

This example shows how to set a port to autonegotiate at only 10 Mbps:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto 10
```

This example shows how to set a port to autonegotiate at only 10 or 100 Mbps:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto 10 100
```

Related Commands

Command	Description
duplex	Specifies the duplex mode of operation.
show interfaces	Displays the statistical information specific to all interfaces or to a specific interface.

storm-control

To enable broadcast, multicast, or unicast storm control and to set threshold levels on an interface, use the **storm-control** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

storm-control {{**broadcast** | **multicast** | **unicast**} **level** {*rising_level* [*falling_level*]} | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]}} | {**action** {**shutdown** | **trap**}}

no storm-control {{**broadcast** | **multicast** | **unicast**} **level**} | {**action** {**shutdown** | **trap**}}

Syntax Description

broadcast	Enables broadcast storm control on the interface.
multicast	Enables multicast storm control on the interface.
unicast	Enables unicast storm control on the interface.
level *rising_level* [*falling_level*]	Specifies the rising and falling suppression levels as a percentage of total bandwidth of the port. • *rising_level*—The rising threshold level for broadcast, multicast, or unicast traffic as a percentage (up to two decimal places) of the bandwidth. The port blocks traffic when the rising threshold is reached. The range is 0.00 to 100.00. • (Optional) *falling_level—T*he falling threshold level as a percentage (up to two decimal places) of the bandwidth. *This value must be less than or equal to the rising suppression value.* The port forwards traffic when traffic drops below this level. If you do not configure a falling suppression level, it is set to the rising suppression level. The range is 0.00 to 100.00. If you set the threshold to the maximum value (100 percent), no limit is placed on the traffic. If you set the threshold to 0.0, all broadcast, multicast, and unicast traffic on that port is blocked.
level bps *bps* [*bps-low*]	Specifies the rising and falling suppression levels as a rate in bits per second at which traffic is received on the port. • **bps** *bps*—The rising threshold level for broadcast, multicast, or unicast traffic in bits per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0. • (Optional) *bps-low*—The falling threshold level in bits per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is 0.0 to 10000000000.0. For **bps** settings, you can use metric suffixes such as k, m, and g for large number thresholds.

level pps *pps* [*pps-low*]	Specifies the rising and falling suppression levels as a rate in packets per second at which traffic is received on the port. • **pps** *pps*—The rising threshold level for broadcast, multicast, or unicast traffic in packets per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0. • (Optional) *pps-low*,—The falling threshold level in packets per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is 0.0 to 10000000000.0. For **pps** settings, you can use metric suffixes such as k, m, and g for large number thresholds.\
action {**shutdown** | **trap**}	Specifies the action to be taken when a storm is detected. The default action is to filter traffic and to not send an Simple Network Management Protocol (SNMP) trap. The keywords have these meanings: • **shutdown**—Error-disables the port during a storm. • **trap**—Sends an SNMP trap when a storm occurs.

Defaults

Broadcast, multicast, and unicast storm control are disabled.

The default action is to filter traffic and to not send an SNMP trap.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Storm control is supported on physical interfaces. When you configure storm control on an interface, it also affects traffic on Ethernet Flow Points (EFPs) configured on the interface.

You can also configure storm control on an EtherChannel. When storm control is configured on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces.

The storm-control suppression level can be entered as a percentage of total bandwidth of the port, as a rate in packets per second at which traffic is received, or as a rate in bits per second at which traffic is received.

When specified as a percentage of total bandwidth, a suppression value of 100 percent means that no limit is placed on the specified traffic type. A value of **level 0 0** means that all broadcast, multicast, or unicast traffic on that port is blocked. Storm control is enabled only when the rising suppression level is less than 100 percent. If no other storm-control configuration is specified, the default action is to filter the traffic causing the storm and to send no SNMP traps.

Note When the storm control threshold for multicast traffic is reached, all multicast traffic except control traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol (CDP) frames, are blocked. However, the switch does not differentiate between routing updates, such as Open Shortest Path First (OSPF) and regular multicast data traffic, so both types of traffic are blocked.

The **trap** and **shutdown** options are independent of each other.

If you configure the action to be taken as shutdown (the port is error-disabled during a storm) when a packet storm is detected, you must use the **no shutdown** interface configuration command to bring the interface out of this state. If you do not specify the **shutdown** action, specify the action as **trap** (the switch generates a trap when a storm is detected).

When a storm occurs and the action is to filter traffic, if the falling suppression level is not specified, the switch blocks all traffic until the traffic rate drops below the rising suppression level. If the falling suppression level is specified, the switch blocks traffic until the traffic rate drops below this level.

When a broadcast storm occurs and the action is to filter traffic, the switch blocks only broadcast traffic.

You can verify the configuration by entering the **show storm-control** privileged EXEC command.

For more information, see the software configuration guide for this release.

Examples

This example shows how to enable broadcast storm control with a 75.5-percent rising suppression level:

This example shows how to enable unicast storm control on a port with an 87-percent rising suppression level and a 65-percent falling suppression level:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# storm-control unicast level 87 65
```

This example shows how to enable broadcast address storm control on a port to a level of 20 percent. When the broadcast traffic exceeds the configured level of 20 percent of the total available bandwidth of the port within the traffic-storm-control interval, the switch drops all broadcast traffic until the end of the traffic-storm-control interval:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# storm-control broadcast level 20
```

Related Commands

Command	Description
show storm-control	Displays broadcast, multicast, or unicast storm control settings on all interfaces or on a specified interface.

switchport

To put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration, use the **switchport** command with no keywords in interface configuration mode. To put an interface in Layer 3 mode, use the **no** form of this command.

switchport

no switchport

Note The **switchport** commands are not available on interfaces with service instances configured.

Syntax Description

This command has no arguments or keywords.

Defaults

By default, all interfaces are in Layer 2 (switching) mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use the **no switchport** command (without parameters) to set the interface to the routed-interface status and to erase all Layer 2 configurations. You must enter the **no switchport** command and then assign an IP address to the routed port.

If an interface is configured as a Layer 3 interface, to process traffic through the CPU, you must first enter the **switchport** command with no keywords before configuring switching characteristics on the port. Then you can enter additional **switchport** commands with keywords, as shown on the pages that follow.

Entering the **no switchport** command shuts the port down and then re-enables it, which might generate messages on the device to which the port is connected.

When you enter the **switchport** (or **no switchport**) command without keywords on an interface, the configuration information for the affected interface might be lost, and the interface returned to its default configuration.

The **switchport** commands are not available on interfaces with service instances configured.

You can verify the switchport status of an interface by entering the **show running-config** privileged EXEC command.

Examples

This example shows how to change an interface from a Layer 2 (switching) port to a Layer 3 (routed) port.

```
Switch(config-if)# no switchport
```

This example shows how to return the port to switching mode:

```
Switch(config-if)# switchport
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
show running-config	Displays the operating configuration.

switchport access vlan

To configure a port as a static-access port, use the **switchport access vlan** command in interface configuration mode. If the switchport mode is set to **access** (by using the **switchport mode** interface configuration command), use this command to set the port to operate as a member of the specified VLAN. To reset the access VLAN mode to the default VLAN for the switch, use the **no** form of this command.

switchport access vlan {*vlan-id* | **dynamic**}

no switchport access vlan

Note This command is not available on interfaces with service instances configured.

Syntax Description

vlan-id	Configure the interface as a static access port with the VLAN ID of the access mode VLAN; the range is 1 to 4094.

Note Although visible in the command-line help, the **dynamic** keyword is not supported.

Defaults

The default access VLAN and trunk interface native VLAN is a VLAN corresponding to the platform or interface hardware.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **no switchport access vlan** command resets the access mode VLAN to the appropriate default VLAN for the device.

The port must be in access mode before the **switchport access vlan** command can take effect.

An access port can be assigned to only one VLAN.

You can verify the configuration by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command and examining information in the Administrative Mode and Operational Mode rows.

Examples

This example shows how to change a Layer 2 interface in access mode to operate in VLAN 2 instead of the default VLAN.

```
Switch(config-if)# switchport access vlan 2
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings.
switchport mode	Configures the VLAN membership mode of a port.

switchport backup interface

To configure Flex Links, a pair of interfaces that provide backup to each other, use the **switchport backup interface** command in interface configuration mode on a Layer 2 interface. To remove the Flex Links configuration, use the **no** form of this command.

switchport backup interface [*interface-id* | **GigabitEthernet** *interface-id* | **Port-channel** *interface-id*] {**mmu primary vlan** *interface-id* | **multicast fast-convergence** | **preemption** {**delay** *delay-time* | **mode**} | **prefer vlan** *vlan-id*}

no switchport backup interface [**GigabitEthernet** *interface-id* | **Port-channel** *interface-id*] {**mmu primary vlan** *interface-id* | **multicast fast-convergence** | **preemption** {**delay** *delay-time* | **mode**} | **prefer vlan** *vlan-id*}

Note This command is not available on interfaces with service instances configured.

Syntax Description

GigabitEthernet	GigabitEthernet port name.
Port-channel	Ethernet Channel interface.
interface-id	Specifies that the Layer 2 interface to act as a backup link to the interface being configured. The interface can be a physical interface or port channel. The port-channel range is 1 to 26.
mmu primary vlan *vlan-id*	MAC-address move update. Configure the MAC move update (MMU) for a backup interface pair, using the MAC-address move update primary VLAN ID. The VLAN range is 1 to 4094.
multicast fast-convergence	Enables multicast Fast-convergence.
preemption	Configures a preemption scheme for a backup interface pair.
delay *delay-time*	(Optional) Specifies a preemption delay; the valid values are 1 to 300 seconds.
mode	Specifies a preemption mode as bandwidth, forced, or off.
prefer vlan *vlan-id*	Specifies that VLANs are carried on the backup interfaces of a Flex Link pair. VLAN ID range is 1 to 4,094.
off	(Optional) Specifies that no preemption occurs from backup to active.
delay *delay-time*	(Optional) Specifies a preemption delay; the valid values are 1 to 300 seconds.

Defaults

The default is to have no Flex Links defined. Preemption mode is off. No preemption occurs. Preemption delay is set to 35 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

With Flex Links configured, one link acts as the primary interface and forwards traffic, while the other interface is in standby mode, ready to begin forwarding traffic if the primary link shuts down. The interface being configured is referred to as the active link; the specified interface is identified as the backup link. The feature provides an alternative to the Spanning Tree Protocol (STP), allowing users to turn off STP and still retain basic link redundancy.

- This command is available only for Layer 2 interfaces.
- You can configure only one Flex Link backup link for any active link, and it must be a different interface from the active interface.
- An interface can belong to only one Flex Link pair. An interface can be a backup link for only one active link. An active link cannot belong to another Flex Link pair.
- A backup link does not have to be the same type (Fast Ethernet or Gigabit Ethernet, for instance) as the active link. However, you should configure both Flex Links with similar characteristics so that there are no loops or changes in behavior if the standby link begins to forward traffic.
- Neither of the links can be a port that belongs to an EtherChannel. However, you can configure two port channels (EtherChannel logical interfaces) as Flex Links, and you can configure a port channel and a physical interface as Flex Links, with either the port channel or the physical interface as the active link.
- If STP is configured on the switch, Flex Links do not participate in STP in all valid VLANs. If STP is not running, be sure that there are no loops in the configured topology.

You can verify your setting by entering the **show interfaces switchport backup** privileged EXEC command.

Examples

This example shows how to configure two interfaces as Flex Links:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport backup interface gigabitethernet0/2
Switch(config-if)# end
```

This example shows how to configure the interface to always preempt the backup:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport backup interface gigabitethernet0/2 preemption forced
Switch(config-if)# end
```

This example shows how to configure the interface preemption delay time:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport backup interface gigabitethernet0/2 preemption delay 150
Switch(config-if)# end
```

This example shows how to configure the interface as the MMU primary VLAN:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport backup interface gigabitethernet0/2 mmu primary vlan 1021
Switch(config-if)# end
```

This example shows how to configure preferred VLANs:

```
Switch(config)# interface gigabitethernet 0/6
Switch(config-if)# switchport backup interface gigabitethernet 0/8 prefer vlan 60,100-120
```

In this example, VLANs 60, and 100 to 120 are configured on the switch:

```
Switch(config)# interface gigabitEthernet 0/6
Switch(config-if)# switchport backup interface gigabitEthernet 0/8 prefer vlan 60,100-120
```

When both interfaces are up, Gi0/6 forwards traffic for VLANs 1 to 50, and Gi0/8 forwards traffic for VLANs 60 and 100 to 120.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/6    GigabitEthernet0/8    Active Up/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

When a Flex Link interface goes down (LINK_DOWN), VLANs preferred on this interface are moved to the peer interface of the Flex Link pair. In this example, if interface Gi0/6 goes down, Gi0/8 carries all VLANs of the Flex Link pair.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/6    GigabitEthernet0/8    Active Down/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

When a Flex Link interface comes up, VLANs preferred on this interface are blocked on the peer interface and moved to the forwarding state on the interface that has just come up. In this example, if interface Gi0/6 comes up, VLANs preferred on this interface are blocked on the peer interface Gi0/8 and forwarded on Gi0/6.

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/6    GigabitEthernet0/8    Active Up/Backup Up

Vlans Preferred on Active Interface: 1-50
Vlans Preferred on Backup Interface: 60, 100-120
```

This example shows how to configure multicast fast-convergence on interface Gi0/11:

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 0/11
Switch(config-if)# switchport backup interface gigabitEthernet 0/12 multicast
fast-convergence
Switch(config-if)# end
```

```
Switch# show interfaces switchport backup detail

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State
------------------------------------------------------------------------
GigabitEthernet0/11   GigabitEthernet0/12   Active Up/Backup Standby
        Preemption Mode  : off
        Multicast Fast Convergence  : On
        Bandwidth : 1000000 Kbit (Gi0/11), 1000000 Kbit (Gi0/12)
        Mac Address Move Update Vlan : auto
```

Related Commands

Command	Description
show interfaces [*interface-id*] **switchport backup**	Displays the configured Flex Links and their status on the switch or for the specified interface.

switchport block

To prevent unknown multicast or unicast packets from being forwarded, use the **switchport block** command in interface configuration mode. To allow forwarding unknown multicast or unicast packets, use the **no** form of this command.

switchport block {**multicast | unicast**}

no switchport block {**multicast | unicast**}

Note This command is not available on interfaces with service instances configured.

Syntax Description

multicast	Specifies that unknown multicast traffic should be blocked. **Note** Only pure Layer 2 multicast traffic is blocked. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.
unicast	Specifies that unknown unicast traffic should be blocked.

Defaults

Unknown multicast and unicast traffic is not blocked.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

By default, all traffic with unknown MAC addresses is sent to all ports. You can block unknown multicast or unicast traffic on protected or nonprotected ports. If unknown multicast or unicast traffic is not blocked on a protected port, there could be security issues.

With multicast traffic, the port blocking feature blocks only pure Layer 2 packets. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.

Blocking unknown multicast or unicast traffic is not automatically enabled on protected ports; you must explicitly configure it.

You can verify your setting by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

For more information about blocking packets, see the software configuration guide for this release.

Examples

This example shows how to block unknown multicast traffic on an interface:

```
Switch(config-if)# switchport block multicast
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.

switchport host

To optimize a Layer 2 port for a host connection, use the **switchport host** command in interface configuration mode. The **no** form of this command has no affect on the system.

switchport host

Note This command is not available on interfaces with service instances configured.

Syntax Description

This command has no arguments or keywords.

Defaults

The default is for the port to not be optimized for a host connection.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

To optimize the port for a host connection, the **switchport host** command sets switch port mode to access, enables spanning tree Port Fast, and disables channel grouping. Only an end station can accept this configuration.

Because spanning tree Port Fast is enabled, you should enter the **switchport host** command only on ports that are connected to a single host. Connecting other switches, hubs, concentrators, or bridges to a fast-start port can cause temporary spanning-tree loops.

Enable the **switchport host** command to decrease the time that it takes to start up packet forwarding.

You can verify your setting by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

Examples

This example shows how to optimize the port configuration for a host connection:

```
Switch(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Switch(config-if)#
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port, including switchport mode.

switchport mode

To configure the VLAN membership mode of a port, use the **switchport mode** command in interface configuration mode. To reset the mode to the default, use the **no** form of this command.

switchport mode {**access** | **trunk**}

no switchport mode

Note This command is not available on interfaces with service instances configured.

Syntax Description

access	Sets the port to access mode (either static-access or dynamic-access depending on the setting of the **switchport access vlan** interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that sends and receives unencapsulated (nontagged) frames. An access port can be assigned to only one VLAN.
trunk	Sets the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router.

Defaults

The default mode is **access**.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

A configuration that uses the **access** or **trunk** keywords takes effect only when you configure the port in the appropriate mode by using the **switchport mode** command. The static-access and trunk configuration are saved, but only one configuration is active at a time.

When you enter **access** mode, the interface changes to permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

When you enter **trunk** mode, the interface changes to permanent trunking mode and negotiates to convert the link into a trunk link even if the interface connecting to it does not agree to the change. If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.

Access ports and trunk ports are mutually exclusive.

You can verify your settings by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command and examining information in the Administrative Mode and Operational Mode rows.

Examples

This example shows how to configure a port for access mode:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
```

This example shows how to configure a port for trunk mode:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode trunk
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport access vlan	Configures a port as a static-access or dynamic-access port.
switchport trunk	Configures the trunk characteristics when an interface is in trunking mode.

switchport trunk

To set the trunk characteristics when the interface is in trunking mode, use the **switchport trunk** command in interface configuration mode. To reset a trunking characteristic to the default, use the **no** form of this command.

switchport trunk {**allowed vlan** *vlan-list* | **native vlan** *vlan-id*}

no switchport trunk {**allowed vlan | native vlan**}

Note This command is not available on interfaces with service instances configured.

Syntax Description

allowed vlan *vlan-list*	Sets the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. See the following *vlan-list* format. The **none** keyword is not valid. The default is **all**.
native vlan *vlan-id*	Sets the native VLAN for sending and receiving untagged traffic when the interface is in 802.1Q trunking mode. The range is 1 to 4094.

The *vlan-list* format is **all | none | [add | remove | except]** *vlan-atom* [**,***vlan-atom...*] where:

- **all** specifies all VLANs from 1 to 4094. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
- **none** means an empty list. This keyword is not allowed on commands that require certain VLANs to be set or at least one VLAN to be set.
- **add** adds the defined list of VLANs to those currently set instead of replacing the list. Valid IDs are from 1 to 4094. You can add extended-range VLANs (VLAN IDs greater than 1005) to the allowed VLAN list.

  Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- **remove** removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 4094; extended-range VLAN IDs are valid.

  Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.) Valid IDs are from 1 to 1005. Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- *vlan-atom* is either a single VLAN number from 1 to 4094 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

Defaults

VLAN 1 is the default native VLAN ID on the port.

The default for all VLAN lists is to include all VLANs.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Native VLANs:

- All untagged traffic received on an IEEE 802.1Q trunk port is forwarded with the native VLAN configured for the port.
- If a packet has a VLAN ID that is the same as the sending-port native VLAN ID, the packet is sent without a tag; otherwise, the switch sends the packet with a tag.
- The **no** form of the **native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

Allowed VLAN:

- To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), and Link Aggregation Control Protocol (LACP) in VLAN 1.
- The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

You can verify your settings by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

Examples

This example shows how to configure VLAN 3 as the default for the port to send all untagged traffic:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk native vlan 3
```

This example shows how to add VLANs 1, 2, 5, and 6 to the allowed list:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

Related Commands

Command	Description
show interfaces switchport	Displays the administrative and operational status of a switching (nonrouting) port.
switchport mode	Configures the VLAN membership mode of a port.

system env temperature threshold alert

To configure the delta value from the shutdown threshold for a high or low alert to be generated, use the **system env temperature threshold alert** command in global configuration mode. To return to the default, use the **no** form of this command.

system env temperature threshold alert {**high** | **low**} *value*

no system env temperature threshold alert {**high** | **low**}

Syntax Description

high	Configures the high temperature threshold when an alert should be sent.
low	Configures the low temperature threshold when an alert should be sent.
value	Specifies the delta value in degrees Celsius from the shutdown threshold for an high or low alert to be generated. The range is from 20 to 40 degrees Celcius.

Defaults

The default value is 10 degrees Celcius. An alert is sent when the temperature is 10 degrees higher or lower than the shutdown threshold.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example sets 15 degrees Celcius as the high value delta from the shutdown threshold so that an alert is sent if the temperature is 15 degrees higher than the shutdown threshold:

```
Switch(config)# system env temperature threshold alert high 15
Switch(config)#
```

Related Commands

Command	Description
show env temperature status	Displays the switch temperature status and thresholds.

test cable-diagnostics tdr

To run the Time Domain Reflector (TDR) feature on an interface, use the **test cable-diagnostics tdr** command in privileged EXEC mode.

test cable-diagnostics tdr interface *interface-id*

Note TDR is supported only on GigabitEthernet 10/100/100 ports.

interface-id	Specifies the interface on which to run TDR.

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can use the TDR feature to diagnose and resolve cabling problems. TDR is supported only on copper Ethernet 10/100 or 10/100/1000 ports. It is not supported on small form-factor pluggable (SFP) module ports or on 10 Gigabit Ethernet ports. For more information about TDR, see the software configuration guide for this release.

After you run TDR by using the **test cable-diagnostics tdr interface** *interface-id* command, use the **show cable-diagnostics tdr interface** *interface-id* privileged EXEC command to display the results.

Examples

This example shows how to run TDR on an interface:

```
Switch# test cable-diagnostics tdr interface gigabitethernet0/2
TDR test started on interface Gi0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

If you enter the **test cable-diagnostics tdr interface** *interface-id* command on an interface that has a link status of up and a speed of 10 or 100 Mbps, these messages appear:

```
Switch# test cable-diagnostics tdr interface gigabitethernet0/3
TDR test on Gi0/9 will affect link state and traffic
TDR test started on interface Gi0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

Related Commands

Command	Description
show cable-diagnostics tdr	Displays the TDR results.

traceroute mac

To display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address, use the **traceroute mac** command in privileged EXEC mode.

traceroute mac [**interface** *interface-id*] {*source-mac-address*} **[interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]

Syntax Description

interface *interface-id*	(Optional) Specifies an interface on the source or destination switch.
source-mac-address	Specifies the MAC address of the source switch in hexadecimal format.
destination-mac-address	Specifies the MAC address of the destination switch in hexadecimal format.
vlan *vlan-id*	(Optional) Specifies the VLAN on which to trace the Layer 2 path that the packets take from the source switch to the destination switch. Valid VLAN IDs are 1 to 4094.
detail	(Optional) Specifies that detailed information appears.

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

When the switch detects a device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and an error message appears.

The **traceroute mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN. If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[ME-3400-24TS] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5                 (2.2.5.5        )  :    Gi0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows how to display the Layer 2 path by using the **detail** keyword:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[ME-3400-24TS] (2.2.6.6)
ME-3400-24TS / 2.2.6.6 :
        Gi0/2 [auto, auto] => Gi0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination switches:

```
Switch# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
Source 0000.0201.0601 found on con6[ME-3400-24TS] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5                 (2.2.5.5        )  :    Gi0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows the Layer 2 path when the switch is not connected to the source switch:

```
Switch# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.0201.0501 found on con5[ME-3400-24TS] (2.2.5.5)
con5 / ME-3400-24TS/ 2.2.5.5 :
        Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows the Layer 2 path when the switch cannot find the destination port for the source MAC address:

```
Switch# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Switch# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

This example shows the Layer 2 path when source and destination switches belong to multiple VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

Related Commands

Command	Description
traceroute mac ip	Displays the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

traceroute mac ip

To display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname, use the **traceroute mac ip** command in privileged EXEC mode.

traceroute mac ip {*source-ip-address* | *source-hostname*} {*destination-ip-address* | *destination-hostname*} [**detail**]

Syntax Description

source-ip-address	Specifies the IP address of the source switch as a 32-bit quantity in dotted-decimal format.
destination-ip-address	Specifies the IP address of the destination switch as a 32-bit quantity in dotted-decimal format.
source-hostname	Specifies the IP hostname of the source switch.
destination-hostname	Specifies the IP hostname of the destination switch.
detail	(Optional) Specifies that detailed information appears.

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

When the switch detects an device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet. When you specify the IP addresses, the switch uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the switch uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the switch sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Switch# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / ME-3400-24TS-/ 2.2.6.6 :
        Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Switch# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5                 (2.2.5.5        )  :    Gi0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

This example shows the Layer 2 path when ARP cannot associate the source IP address with the corresponding MAC address:

```
Switch# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

Related Commands

Command	Description
shutdown	Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

udld

To enable aggressive or normal mode in the UniDirectional Link Detection (UDLD) and to set the configurable message timer, use the **udld** command in global configuration mode. To disable aggressive or normal mode UDLD on all fiber-optic ports, use the **no** form of the command.

udld {**aggressive** | **enable** | **message time** *message-timer-interval*}

no udld {**aggressive** | **enable** | **message**}

Syntax Description

aggressive	Enables UDLD in aggressive mode on all fiber-optic interfaces.
enable	Enables UDLD in normal mode on all fiber-optic interfaces.
message time *message-timer-interval*	Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is 7 to 90 seconds.

Defaults

UDLD is disabled on all interfaces.

The message timer is set at 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the "Understanding UDLD" section in the software configuration guide for this release.

If you change the message time between probe packets, you are making a trade-off between the detection speed and the CPU load. By decreasing the time, you can make the detection-response faster but increase the load on the CPU.

This command affects fiber-optic interfaces only. Use the **udld** interface configuration command to enable UDLD on other interface types.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command to reset all interfaces shut down by UDLD
- The **shutdown** and **no shutdown** interface configuration commands
- The **no udld enable** global configuration command followed by the **udld** {**aggressive** | **enable**} global configuration command to re-enable UDLD globally

- The **no udld port** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to re-enable UDLD on the specified interface
- The **errdisable recovery cause udld** and **errdisable recovery interval** *interval* global configuration commands to automatically recover from the UDLD error-disabled state

You can verify your setting by entering the **show udld** privileged EXEC **command**.

Examples

This example shows how to enable UDLD on all fiber-optic interfaces:

```
Switch(config)# udld enable
```

Related Commands

Command	Description
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command.
udld reset	Resets all interfaces shut down by UDLD and permits traffic to again pass through.

udld port

To enable the UniDirectional Link Detection (UDLD) on an individual interface or prevent a fiber-optic interface from being enabled by the **udld** global configuration command, use the **udld port** command in interface configuration mode. To return to the **udld** global configuration command setting or to disable UDLD if entered for a nonfiber-optic port, use the **no** form of this command.

udld port [**aggressive | disable**]

no udld port [**aggressive | disable**]

Syntax Description

aggressive	Enables UDLD in aggressive mode on the specified interface.
disable	Disables UDLD on this interface despite the global UDLD setting.

Defaults

On fiber-optic interfaces, UDLD is not enabled, not in aggressive mode, and not disabled. For this reason, fiber-optic interfaces enable UDLD according to the state of the **udld enable** or **udld aggressive** global configuration command.

On nonfiber-optic interfaces, UDLD is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52EY	This command was introduced.

Usage Guidelines

A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch. If the port is a user network interface (UNI) or enhanced network interface (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **udld port** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the “Configuring UDLD” chapter in the software configuration guide for this release.

To enable UDLD in normal mode, use the **udld port** interface configuration command. To enable UDLD in aggressive mode, use the **udld port aggressive** interface configuration command.

Use the **no udld port** command on fiber-optic ports to return control of UDLD to the **udld enable** global configuration command or to disable UDLD on nonfiber-optic ports.

Use the **udld port aggressive** command on fiber-optic ports to override the setting of the **udld enable** or **udld aggressive** global configuration command. Use the **no** form on fiber-optic ports to remove this setting and to return control of UDLD enabling to the **udld** global configuration command or to disable UDLD on nonfiber-optic ports.

For UDLD to peer with a neighbor on a port that has an Ethernet Virtual Connection (EVC) EFP service instance configured, you need to enter the **l2 protocol peer udld** service-instance configuration command on the service instance.

If the switch software detects a small form-factor pluggable (SFP) module change and the port changes from fiber optic to nonfiber optic or the reverse, all configurations are maintained.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command to reset all interfaces shut down by UDLD.
- The **shutdown** and **no shutdown** interface configuration commands.
- The **no udld enable** global configuration command followed by the **udld** {**aggressive** | **enable**} global configuration command to re-enable UDLD globally.
- The **no udld port** interface configuration command followed by the **udld port or udld port aggressive** interface configuration command to re-enable UDLD on the specified interface.
- The **errdisable recovery cause udld** and **errdisable recovery interval** *interval* global configuration commands to automatically recover from the UDLD error-disabled state.

You can verify your settings by entering the **show running-config** or the **show udld** *interface* privileged EXEC command.

Examples

This example shows how to enable UDLD on an port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# udld port
```

This example shows how to configure UDLD peering on an EFP service instance:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# udld port
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan none
Switch(config-if)# service instance 1 Ethernet
Switch(config-if-srv)# encapsulation untagged
Switch(config-if-srv)# l2protocol peer udld
Switch(config-if-srv)# bridge-domain 10
Switch(config-if-srv)# end
```

This example shows how to disable UDLD on a fiber-optic interface despite the setting of the **udld** global configuration command:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no udld port
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld reset	Resets all interfaces shut down by UDLD and permits traffic to again pass through.

udld reset

To reset all interfaces disabled by the UniDirectional Link Detection (UDLD) and permit traffic to begin passing through them again, use the **udld reset** command in privileged EXEC mode. Other enabled features, such as spanning tree and Port Aggregation Protocol (PAgP), still have their normal effects.

udld reset

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and are disabled for the same reason if the problem has not been corrected.

You can verify your setting by entering the **show udld** privileged EXEC command.

Examples

This example shows how to reset all interfaces disabled by UDLD:

```
Switch# udld reset
1 ports shutdown by UDLD were reset.
```

Related Commands

Command	Description
show running-config	Displays the operating configuration.
show udld	Displays UDLD administrative and operational status for all ports or the specified port.
udld	Enables aggressive or normal mode in UDLD or sets the configurable message timer time.
udld port	Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command.

uni count

To set the user-network interface (UNI) count for an Ethernet virtual connection (EVC), use the **uni count** command in EVC configuration mode. To return to the default setting, use the **no** form of this command.

uni count *value* [**multipoint**]

no uni count

Syntax Description

value	Sets the number of UNIs in the EVC. The range is from 2 to 1024. The default is 2.
multipoint	(Optional) Selects point-to-multipoint service. This keyword is visible only when you enter a **uni count** value of 2. • If you do not enter a value or if you enter 1 or 2, the service defaults to point-to-point service. If you enter 2, you can configure point-to-multipoint service. • If you enter a **uni count** value of 3 or greater, the service is point-to-multipoint.

Defaults

The default UNI count is 2. The default service, if you do not enter a UNI count, is point-to-multipoint.

Command Modes

EVC configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The UNI count determines the type of service in the EVC.

- If the command is not entered, the UNI count defaults to 2 and the service defaults to point-to-point service.
- If you manually enter a value of 2, you can leave the service at the default or can configure point-to-multipoint service by entering the **multipoint** keyword.
- If you enter a value of 3 or greater, the service is point-to-multipoint.

You should know the correct number of maintenance end points (MEPs) in the domain. If you enter a UNI count value greater than the actual number of endpoints, the UNI status shows as partially active even if all endpoints are up. If you enter a UNI count less than the actual number of endpoints, UNI status shows as active, even if all endpoints are not up.

Caution Configuring a UNI count does not prevent you from configuring more endpoints than the configured count. For example, if you configure a UNI count of five, but you create ten MEPs, any five MEPs in the domain can go down without the status changing to Partially Active.

Examples

This example shows how to a UNI count of two with point-to-multipoint service:

```
Switch(config)# ethernet evc test1
Switch(config-evc)# uni count 2 multipoint
```

Related Commands

Command	Description
ethernet evc *evc-id*	Defines an EVC and enters EVC configuration mode.

uni-vlan

To configure a VLAN as a user network interface (UNI) community or isolated VLAN, use the **uni-vlan** command in VLAN configuration mode. UNIs on a switch that are assigned to a community VLAN can exchange packets with one another.

uni-vlan {**community** | **isolated**}

no uni-vlan

Note This command has no effect on the switch. All ports on the switch are network node interfaces (NNIs), which can always exchange packets with one another.

Syntax Description

community	Designate the UNI-ENI VLAN as a community VLAN.
isolated	Designate the UNI-ENI VLAN as an isolated VLAN.

Defaults

The default VLAN configuration is UNI-ENI isolated VLAN.

Command Modes

VLAN configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

This command has no effect on the switch because all ports on the switch are NNIs.

Related Commands

Command	Description
show interfaces status	Displays the status of interfaces, including the VLANs to which they belong.

violate-action

To set actions for a policy-map class for packets that exceed the peak information rate (PIR), use the **violate-action** command in policy-map class police configuration mode. To cancel the action or to return to the default action, use the **no** form of this command.

violate-action {**drop** | **set-cos-transmit** *new cos-value* | **set-discard-class-transmit** *new discard-value* | **set-dscp-transmit** *new dscp-value* | **set-mpls-exp-imposition-transmit** *new-imposition-exp-value* | **set-mpls-exp-topmost transmit** *new-topmost-exp-value* | **set-prec-transmit value** *new prec-value* | **set-qos-transmit value** *new qos-value*| **transmit**}

no violate-action {**drop** | **set-cos-transmit** *new cos-value* | **set-discard-class-transmit** *new discard-value* | **set-dscp-transmit** *new dscp-value* | **set-mpls-exp-imposition-transmit** *new-imposition-exp-value* | **set-mpls-exp-topmost transmit** *new-topmost-exp-value* | **set-prec-transmit value** *new prec-value* | **set-qos-transmit value** *new qos-value*| **transmit**}

Syntax Description

drop	Drops the packet.
set-cos-transmit *new-cos-value*	Sets a new class of service (CoS) value for the packet and send the packet. The range for the new CoS value is 0 to 7.
set-discard-class-transmit *new discard-value*	Sets a new discard-class value for the packet and send the packet. The range for the value is 0 to 7.
set-dscp-transmit *new-dscp-value*	Sets a new Differentiated Services Code Point (DSCP) value for the packet and send the packet. The range for the new DCSP value is 0 to 63.
set-mpls-exp-imposition transmit *new-imposition-exp-value*	Sets an MPLS label using the new MPLS EXP value at tag imposition, and send the packet. The range is 0 to 7.
set-mpls-exp-topmost transmit *new-topmost-exp-value*	Sets an MPLS label using the new MPLS EXP value for the topmost (outer) MPLS label, and send the packet. The range is 0 to 7.
set-prec-transmit *new-precedence-value*	Sets a new IP precedence value for the packet and send the packet. The range for the new IP precedence value is 0 to 7.
set-qos-transmit *qos-group-value*	Sets a new quality of service (QoS) group value for the packet and send the packet. The range for the new QoS value is 0 to 99.
transmit	(Optional) Sends the packet unmodified.

Defaults

The default action is to drop the packet.

Command Modes

Policy-map class police configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You configure violate actions for packets that exceed the peak information rate (PIR).

The switch also supports marking multiple QoS parameters for the same class and simultaneously configuring conform-action, exceed action, and violate-action marking.

Access policy-map class police configuration mode by entering the **police** policy-map class command. See the **police** command for more information.

You can use this command to set one or more violate actions for a traffic class.

For both individual and aggregate policers, if you do not configure a violate action, by default the violate class is assigned the same action as the exceed action.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Examples

This example shows how configure multiple actions in a policy map that sets a committed information rate of 5000000 bits per second (b/s) and a peak rate of 8000000 b/s:

```
Switch(config)# policy-map map1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police cir 5000000 pir 8000000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-dscp-transmit 24
Switch(config-pmap-c-police)# violate-action drop
Switch(config-pmap-c-police)# end
```

Related Commands

Command	Description
class	Defines a traffic classification match criteria for the specified class-map name.
conform-action	Defines the action to take on traffic that conforms to the CIR.
exceed-action	Defines the action to take on traffic between the conform rate and the conform rate plus the exceed burst.
police	Defines a policer for classified traffic.
policy-map	Creates or modifies a policy map that can be attached to multiple ports to specify a service policy.
show policy-map	Displays quality of service (QoS) policy maps.

vlan

To create a VLAN and to enter VLAN configuration mode, use the **vlan** command with a VLAN ID in global configuration mode. To delete the VLAN, use the **no** form of this command. Configuration information for normal-range VLANs (VLAN IDs 1 to 1005) is always saved in the VLAN database as well as in the switch running configuration file. Configuration information for extended-range VLANs (VLAN IDs greater than 1005), are saved only in the switch running configuration file. You can save configurations in the switch startup configuration file by entering the **copy running-config startup-config** privileged EXEC command.

vlan *vlan-id*

no vlan *vlan-id*

Syntax Description

vlan-id	ID of the VLAN to be added and configured. For *vlan-id*, the range is 1 to 4094. You can enter a single VLAN ID, a series of VLAN IDs separated by commas, or a range of VLAN IDs separated by hyphens.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Extended-range VLANs (VLAN IDs 1006 to 4094) are not added to the VLAN database, but all VLAN configurations are saved in the running configuration, and you can save them in the switch startup configuration file.

Entering the **vlan** command with a VLAN ID enables VLAN configuration mode. If you enter an invalid VLAN ID, you receive an error message and do not enter VLAN configuration mode.

When you enter the VLAN ID of an existing VLAN, you do not create a new VLAN, but you can modify VLAN parameters for that VLAN. The specified VLANs are added or modified when you exit VLAN configuration mode. Only the **shutdown** command (for VLANs 1 to 1005) takes effect immediately.

These configuration commands are available in VLAN configuration mode. The **no** form of each command returns the characteristic to its default state.

Note Although all commands are visible, the only VLAN configuration command that is supported on extended-range VLANs is **mtu** *mtu-size*. For extended-range VLANs, all other characteristics must remain at the default state.

Note The switch supports only Ethernet VLANs. You can configure parameters for FDDI and Token Ring VLANs and view the results in the vlan.dat file, but these parameters are not used.

- **are** *are-number*: defines the maximum number of all-routes explorer (ARE) hops for TrCRF VLANs. The range is 0 to 13. The default is 7.
- **backupcrf {enable | disable}**: specifies the backup CRF mode for TrCRF VLANs.
- **bridge** {*bridge-number*| **type**}: specifies the logical distributed source-routing bridge, the bridge that interconnects all logical rings having this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TrBRF VLANs. The range is 0 to 15. The default bridge number is 0.
- **exit**: applies changes, increments the VLAN database revision number (VLANs 1 to 1005 only), and exits VLAN configuration mode.
- **media**: defines the VLAN media type.
  - **ethernet** is Ethernet media type (the default).
  - **fddi** is FDDI media type.
  - **fd-net** is FDDI network entity title (NET) media type.
  - **tokenring** is Token Ring media type or TrCRF.
  - **tr-net** is Token Ring network entity title (NET) media type or TrBRF media type.
- **mtu** *mtu-size*: specifies the maximum transmission unit (MTU) (packet size in bytes). The range is 1500 to 18190. The default is 1500 bytes.
- **name** *vlan-name*: names the VLAN with an ASCII string from 1 to 32 characters that must be unique within the administrative domain. The default is *VLANxxxx* where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number.
- **no**: negates a command or returns it to the default setting.
- **parent** *parent-vlan-id*: specifies the parent VLAN of an existing FDDI, Token Ring, or TrCRF VLAN. The range is 0 to 1005. The default parent VLAN ID is 0 (no parent VLAN).
- **ring** *ring-number*: defines the logical ring for an FDDI, Token Ring, or TrCRF VLAN. The range is 1 to 4095.
- **said** *said-value*: specifies the security association identifier (SAID) as documented in IEEE 802.10. The range is 1 to 4294967294, and the number must be unique within the administrative domain. The default value is 100000 plus the VLAN ID number.
- **shutdown**: shuts down VLAN switching on the VLAN. This command takes effect immediately. Other commands take effect when you exit VLAN configuration mode.
- **state**: specifies the VLAN state:
  - **active** means the VLAN is operational (the default).
  - **suspend** means the VLAN is suspended. Suspended VLANs do not pass packets.
- **ste** *ste-number*: defines the maximum number of spanning-tree explorer (STE) hops for TrCRF VLANs. The range is 0 to 13. The default is 7.
- **stp type**: defines the spanning-tree type for FDDI-NET, Token Ring-NET, or TrBRF VLANs.
  - **ieee** for IEEE Ethernet STP running source-route transparent (SRT) bridging.
  - **ibm** for IBM STP running source-route bridging (SRB).

  - **auto** for STP running a combination of source-route transparent bridging (IEEE) and source-route bridging (IBM).

- **tb-vlan1** *tb-vlan1-id* and **tb-vlan2** *tb-vlan2-id*: specifies the first and second VLAN to which this VLAN is translationally bridged. Translational VLANs translate FDDI or Token Ring to Ethernet, for example. The range is 0 to 1005. If no value is specified, 0 (no transitional bridging) is assumed.

You can verify your setting by entering the **show vlan** privileged EXEC command.

Examples

This example shows how to add an Ethernet VLAN with default media characteristics. The default includes a *vlan-name* of *VLANxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number. The default **media** option is **ethernet**; the **state** option is **active**. The default *said-value* variable is 100000 plus the VLAN ID; the *mtu-size* variable is 1500; the **stp-type** option is **ieee**. When you enter the **exit** VLAN configuration command, the VLAN is added if it did not already exist; otherwise, this command does has no affect.

This example shows how to create a new VLAN with all default characteristics and enter config-vlan mode:

```
Switch(config)# vlan 200
Switch(config-vlan)# exit
```

Related Commands

Command	Description
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified).

vlan access-map

To create or modify a VLAN map entry for VLAN packet filtering and to enter VLAN access-map configuration mode, use the **vlan access-map** command in global configuration mode. To delete a VLAN map entry, use the **no** form of this command. Use the **vlan filter** interface configuration command to apply a VLAN map to one or more VLANs.

vlan access-map *name* [*number*]

no vlan access-map *name* [*number*]

Syntax Description

name	Name of the VLAN map.
number	(Optional) The sequence number of the map entry that you want to create or modify (0 to 65535). If you are creating a VLAN map and the sequence number is not specified, it is automatically assigned in increments of 10, starting from 10. This number is the sequence to insert to, or delete from, a VLAN access-map entry.

Defaults

There are no VLAN map entries and no VLAN maps applied to a VLAN.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

In global configuration mode, use this command to create or modify a VLAN map. This entry changes the mode to VLAN access-map configuration, where you can use the **match** access-map configuration command to specify the access lists for IP or non-IP traffic to match and use the **action** command to set whether a match causes the packet to be forwarded or dropped.

In VLAN access-map configuration mode, these commands are available:

- **action**: sets the action to be taken (forward or drop).
- **default**: sets a command to its defaults
- **exit**: exits from VLAN access-map configuration mode
- **match**: sets the values to match (IP address or MAC address).
- **no**: negates a command or set its defaults

When you do not specify an entry number (sequence number), it is added to the end of the map.

There can be only one VLAN map per VLAN and it is applied as packets are received by a VLAN.

You can use the **no vlan access-map** *name* [*number*] command with a sequence number to delete a single entry.

In global configuration mode, use the **vlan filter** interface configuration command to apply the map to one or more VLANs.

Note For more information about VLAN map entries, see the software configuration guide for this release.

Examples

This example shows how to create a VLAN map named *vac1* and apply matching conditions and actions to it. If no other entries already exist in the map, this will be entry 10.

```
Switch(config)# vlan access-map vac1
Switch(config-access-map)# match ip address acl1
Switch(config-access-map)# action forward
```

This example shows how to delete VLAN map *vac1*:

```
Switch(config)# no vlan access-map vac1
```

Related Commands

Command	Description
action	Sets the action for the VLAN access map entry.
match (access-map configuration)	Sets the VLAN map to match packets against one or more access lists.
show vlan access-map	Displays information about a particular VLAN access map or all VLAN access maps.
vlan filter	Applies the VLAN access map to one or more VLANs.

vlan dot1q tag native

To enable tagging of native VLAN frames on all IEEE 802.1Q trunk ports, use the **vlan dot1q tag native** command in global configuration mode. To return to the default setting, use the **no** form of this command.

vlan dot1q tag native

no vlan dot1q tag native

Syntax Description

This command has no arguments or keywords.

Defaults

IEEE 802.1Q native VLAN tagging is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When enabled, native VLAN packets going out all 802.1Q trunk ports are tagged.

When disabled, native VLAN packets going out all 802.1Q trunk ports are not tagged.

Layer 2 control packets that are normally untagged, such as MSTP and CDP, are still sent out untagged.

Examples

This example shows how to enable 802.1Q tagging on native VLAN frames:

```
Switch# configure terminal
Switch (config)# vlan dot1q tag native
Switch (config)# end
```

You can verify your settings by entering the **show vlan dot1q tag native** privileged EXEC command.

Related Commands

Command	Description
show vlan dot1q tag native	Displays 802.1Q native VLAN tagging status.

vlan filter

To apply a VLAN map to one or more VLANs, use the **vlan filter** command in global configuration mode. To remove the map, use the **no** form of this command.

vlan filter *mapname* **vlan-list** {*list* | **all**}

no vlan filter *mapname* **vlan-list** {*list* | **all**}

Syntax Description

mapname	Name of the VLAN map entry.
list	The list of one or more VLANs in the form tt, uu-vv, xx, yy-zz, where spaces around commas and dashes are optional. The range is 1 to 4094.
all	Removes the filter from all VLANs.

Defaults

There are no VLAN filters.

Command Modes

Global configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

To avoid accidentally dropping too many packets and disabling connectivity in the middle of the configuration process, we recommend that you completely define the VLAN access map before applying it to a VLAN.

You can verify your settings by entering the **show vlan filter** privileged EXEC command.

For more information about VLAN map entries, see the software configuration guide for this release.

Examples

This example applies VLAN map entry *map1* to VLANs 20 and 30:

```
Switch(config)# vlan filter map1 vlan-list 20, 30
```

This example shows how to delete VLAN map entry *mac1* from VLAN 20:

```
Switch(config)# no vlan filter map1 vlan-list 20
```

Related Commands

Command	Description
show vlan access-map	Displays information about a particular VLAN access map or all VLAN access maps.
show vlan filter	Displays information about all VLAN filters or about a particular VLAN or VLAN access map.
vlan access-map	Creates a VLAN map entry for VLAN packet filtering.

vpn id

To configure the virtual private network (VPN) number for a virtual forwarding infrastructure (VFI) interface, use the **vpn id** command in VFI configuration mode. To remove the VPN ID from the VFI, use the **no** form of this command.

vpn id *vpn-number*

no vpn id *vpn-number*

Syntax Description

vpn-number	The VPN ID for the VFI interface to use. The range is from 1 to 4294967295.

Defaults

The VPN ID is not configured.

Command Modes

VFI configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You create a VFI and enter VFI configuration mode by entering the **l2 vfi** global configuration command.

You must enter a VPN ID to configure the VFI. Some VFI configuration mode keywords are not visible until you enter a VPN ID. When you enter a **vpn id** *vpn-number,* these additional VFI configuration commands are available:

- **neighbor** *remote-peer-IP-address* **encapsulation mpls**: configures the IP address of the remote peer to become a member of the VPLS configured by the VFI and sets the MPLS encapsulation type.
- **shutdown**: shuts down the VFI interface.

The switch supports a total of 26 VPN routing and forwarding instances (VRFs) and VPNs.

You can verify the configuration by entering the **show vfi** user EXEC command.

Examples

This example shows how to configure a VPLS (VFI *abc*) on a provider edge (PE) switch and assign it to VPN *123*:

```
Switch(config)# l2 vfi abc manual
Switch(config-vfi)# vpn id 123
Switch(config-vfi)# neighbor 20.0.0.1 encapsulation mpls
Switch(config-vfi)# exit
```

Related Commands

Command	Description
l2 vfi	Creates a VFI and enters VFI configuration mode.
show vfi	Displays information about a VFI.

xconnect

to route a Layer 2 packets over a specified point-to-point VC by using Ethernet over multiprotocol label switching (EoMPLS), use the **xconnect** command in interface configuration mode at customer-edge or service provider-edge ingress and egress Ethernet ports or on VLAN interfaces with a destination and virtual-connection (VC) ID. You can also bind the VC to a pseudowire. To route Layer 2 packets over a hierarchical virtual private LAN switching (H-VPLS) VFI between the edge devices, use the command with a virtual forwarding infrastructure (VFI) name. To delete the VC or VFI connection, use the **no** form of this command on both edge devices.

xconnect *destination vc-id* {**encapsuluation mpls** [**pw-class** *pw-class-name*]}

no xconnect

Syntax Description

destination	The destination label distribution protocol (LDP) IP address of the remote provider edge device. The IP address cannot be an IP address on the route on which the command is entered.
vc-id	Assigns a virtual connection identifier (VC ID) for the virtual connection between the two peer provider edge devices. The range is 1 to 4294967295.
encapsuluation mpls	Specifies the MPLS data encapsulation method.
pw-class *pw-class-name*	(Optional) Specifies the pseudowire class for advanced configuration.

Defaults

There are no point-to-point connections configured.

When configured, the attachment circuit is not bound to the pseudowire.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

An MPLS VC runs across an MPLS cloud to connect Ethernet interfaces on two provider edge devices at each edge of the service provider network. You must enter the command at the PE device at each edge of the service provider network to establish a bidirectional virtual connection, which consists of two unidirectional label-switched paths (LSPs). A VC is not established if not properly defined from both ends.

For the *destination* parameter, specify the LDP IP address of the other PE device; do not specify the IP address of the device on which you are entering the command.

The *vc-id* must be unique for each pair of provider edge devices. Therefore, in large networks, you should keep track of the VC ID assignments to ensure that a VC ID is not assigned more than once.

For H-VPLS, you create the VFI and enter VFI configuration mode by entering the **l2 vfi** *vfi-name* global configuration command.

You can attach a VFI to a VLAN or to multiple Ethernet ports. The switch does not allow switching VLAN and port interfaces through the same VFI.

The **pw-class** keyword with the *pw-class-name* value binds the xconnect configuration of an attachment circuit to a specific pseudowire class. In this way, the pseudowire class configuration serves as a template that contains settings used by all attachment circuits bound to it with the xconnect command.

To configure the pseudowire class, use the **pseudowire-class** global configuration command to enter pseudo-wire class configuration mode. See the IOS documentation for this command.

http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_m4.html#wp1015442

The switch supports only the **encapsulation mpls** and **preferred-path** options in pseudo-wire configuration mode.

You can verify the configuration by entering the **show mplsl2 transport vc** privileged EXEC command.

Examples

This example shows how to establish an Ethernet over MPLS (EoMPLS) tunnel between the PE1 VLAN 3 interface and the PE2 VLAN 4 interface. PE1 has IP address 10.0.0.1/32 that PE2 discovers through routing and PE2 has IP address 20.0.0.1/32 that PE1 discovers through routing.

At the PE1 interface:

```
Switch(config)# interface vlan 3
Switch(config-if)# xconnect 20.0.0.1 123 encapsulation mpls
```

At the PE2 interface:

```
Switch(config)# interface vlan 4
Switch(config-if)# xconnect 10.0.0.1 123 encapsulation mpls
```

This example shows how to configure a pseudowire class named *vc-class* and then configure xconnect service for an interface by binding the interface to the pseudowire named *123* with a remote peer *10.0.3.201*. The configuration uses the settings in the pseudowire class.

```
Switch (config)# pseudowire-class vc-class
Switch (config-pw-class)# encapsulation mpls
Switch (config-pw-class)# preferred-path interface tunnel 100
Switch (config-pw-class)# exit
Switch(config)# interface Gigabit Ethernet 1/0/1
Switch(config-if)# xconnect 10.0.3.201 123 pw-class vc-class
```

This example shows how to create VFI *abc* and attach it to a VLAN interface. You need to configure the PE devices at both edges of the MPLS network this way:

```
Switch(config)# l2 vfi abc manual
Switch(config-vfi)# vpn id 123
Switch(config-vfi)# neighbor 10.0.0.1 encapsulation mpls
Switch(config-vfi)# exit
Switch(config)# interface vlan 4
Switch(config-if)# xconnect vfi abc encapsulation mpls
```

Related Commands

Command	Description
l2 vfi	Configures a VFI for implementing VPLS over an MPLS backbone.
show mpls l2transport vc	Displays information about the EoMPLS VCs that have been enabled to route Layer 2 packets on a device.

APPENDIX A

Cisco ME 3800X and ME 3600X Switch Boot Loader Commands

This appendix describes the boot loader commands on the Cisco ME 3800X and ME 3600X switch. During normal boot loader operation, you are not presented with the boot loader command-line prompt. You gain access to the boot loader command line if the switch is set to manually boot, if an error occurs during power-on self-test (POST) DRAM testing, or if an error occurs while loading the operating system (a corrupted Cisco IOS image). You can also access the boot loader if you have lost or forgotten the switch password.

Note The default switch configuration allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process while the switch is powering up and then entering a new password. The password recovery disable feature allows the system administrator to protect access to the switch password by disabling part of this functionality and allowing the user to interrupt the boot process only by agreeing to set the system back to the default configuration. With password recovery disabled, the user can still interrupt the boot process and change the password, but the configuration file (config.text) and the VLAN database file (vlan.dat) are deleted. For more information, see the software configuration guide for this release.

You can access the boot loader through a switch console connection at 9600 bps. Disconnect and then reconnect the switch power cord. After the switch performs POST, the switch begins the autoboot process. The boot loader prompts the user for a break key character during the boot-up sequence, as shown in this example:

```
***** The system will autoboot in 5 seconds *****

Send "break character" to prevent autobooting.
```

The break key character is different for each operating system.

- On a SUN work station running UNIX, Ctrl-C is the break key.
- On a PC running Windows 2000, Ctrl-Break is the break key.

Cisco TAC has tabulated break keys for most common operating systems and has provided an alternative break key sequence for terminal emulators that do not support the break keys. To view this table, see:

http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a0080174a34.shtml

When you enter the break key, the boot loader *switch:* prompt appears.

The boot loader performs low-level CPU initialization, performs POST, and loads a default operating system image into memory.

arp

To display the contents the Address Resolution Protocol (ARP) table, use the **arp** command in boot loader mode.

arp [*ip_address*]

Syntax Description

ip_address	(Optional) Show the ARP table or the mapping for a specific IP address.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The ARP table has the IP-address-to-MAC-address mappings.

Examples

This example shows how to display the ARP table:

```
switch: arp 172.20.136.8
arp'ing 172.20.136.8...
172.20.136.8 is at 00:1b:78:d1:25:ae, via port 0
```

boot

To load and boot an executable image and to enter the command-line interface, use the **boot** command in boot loader mode.

boot [**-post** | **-n** | **-p** | *flag*] *filesystem***:/***file-url* ...

Syntax Description

-post	(Optional) Runs the loaded image with an extended or comprehensive power-on self-test (POST). Using this keyword causes POST to take longer to complete.
-n	(Optional) Pauses for the Cisco IOS debugger immediately after launching.
-p	(Optional) Pauses for the JTAG debugger right after loading the image.
*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/*file-url*	(Optional) Path (directory) and name of a bootable image. Separate image names with a semicolon.

Defaults

The switch attempts to automatically boot the system by using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable image it can by performing a recursive, depth-first search throughout the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

When you enter the **boot** command without any arguments, the switch attempts to automatically boot the system by using the information in the BOOT environment variable, if any. If you supply an image name for the *file-url* variable, the **boot** command attempts to boot the specified image.

When you set boot loader **boot** command options, they are executed immediately and apply only to the current boot loader session. These settings are not saved for the next boot operation.

Filenames and directory names are case sensitive.

Examples

This example shows how to boot the switch using the *new-image.bin* image:

```
switch: boot flash:/new-images/new-image.bin
```

After entering this command, you are prompted to start the setup program.

Related Commands

Command	Description
set	Sets the BOOT environment variable to boot a specific image when the **BOOT** keyword is appended to the command.

cat

To display the contents of one or more files, use the **cat** command in boot loader mode.

cat *filesystem*:*/file-url ...*

Syntax Description

filesystem:	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	Path (directory) and name of the files to display. Separate each filename with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

Examples

This example shows how to display the contents of two files:

```
switch: cat flash:/new-images/info flash:env_vars
version_suffix: image-name
version_directory: image-name
image_name: image-name.bin
ios_image_file_size: 63984644
total_image_file_size: 8133632
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: me340x
info_end:
BAUD=57600
MANUAL_BOOT=no
```

Related Commands

Command	Description
more	Displays the contents of one or more files.
type	Displays the contents of one or more files.

copy

To copy a file from a source to a destination, use the **copy** command in boot loader mode.

copy [**-b** *block-size*] *filesystem***:/***source-file-url filesystem***:/***destination-file-url*

Syntax Description

-b *block-size*	(Optional) This option is used only for internal development and testing.
*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/*source-file-url*	Path (directory) and filename (source) to be copied.
/*destination-file-url*	Path (directory) and filename of the destination.

Defaults

The default block size is 4 KB.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 45 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

If you are copying a file to a new directory, the directory must already exist.

Examples

This example show how to copy a file at the root:

```
switch: copy flash:test1.text flash:test4.text
.
File "flash:test1.text" successfully copied to "flash:test4.text"
```

You can verify that the file was copied by entering the **dir** *filesystem***:** boot loader command.

Related Commands

Command	Description
delete	Deletes one or more files from the specified file system.

delete

To delete one or more files from the specified file system, use the **delete** command in boot loader mode.

delete *filesystem***:/***file-url* ...

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/*file-url*	Path (directory) and filename to delete. Separate each filename with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

The switch prompts you for confirmation before deleting each file.

Examples

This example shows how to delete two files:

```
switch: delete flash:test2.text flash:test5.text
Are you sure you want to delete "flash:test2.text" (y/n)?y
File "flash:test2.text" deleted
Are you sure you want to delete "flash:test5.text" (y/n)?y
File "flash:test2.text" deleted
```

You can verify that the files were deleted by entering the **dir flash:** boot loader command.

Related Commands

Command	Description
copy	Copies a file from a source to a destination.

dir

To display a list of files and directories on the specified file system, use the **dir** command in boot loader mode.

dir *filesystem***:***/file-url* ...

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	(Optional) Path (directory) and directory name whose contents you want to display. Separate each directory name with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Directory names are case sensitive.

Examples

This example shows how to display the files in flash memory:

```
switch: dir flash:

Directory of flash:/

    3  -rwx        1839   Mar 01 2002 00:48:15  config.text
   11  -rwx        1140   Mar 01 2002 04:18:48  vlan.dat
   21  -rwx          26   Mar 01 2002 00:01:39  env_vars
    9  drwx         768   Mar 01 2002 23:11:42  html
   16  -rwx        1037   Mar 01 2002 00:01:11  config.text
   14  -rwx        1099   Mar 01 2002 01:14:05  homepage.htm
   22  -rwx          96   Mar 01 2002 00:01:39  system_env_vars
   17  drwx        192    Mar 06 2002 23:22:03  image-name


15998976 bytes total (6397440 bytes free)
```

Table A-1 describes the fields in the display.

Table A-1 dir Field Descriptions

Field	Description
2	Index number of the file.
-rwx	File permission, which can be any or all of these: • d—directory • r—readable • w—writable • x—executable
1644045	Size of the file.
<date>	Last modification date.
env_vars	Filename.

Related Commands

Command	Description
mkdir	Creates one or more directories.
rmdir	Removes one or more directories.

flash_init

To initialize the flash file system, use the **flash_init** command in boot loader mode.

flash_init

Syntax Description

This command has no arguments or keywords.

Defaults

The flash file system is automatically initialized during normal system operation.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

During the normal boot process, the flash file system is automatically initialized.

Use this command to manually initialize the flash file system. For example, you use this command during the recovery procedure for a lost or forgotten password.

format

To format the specified file system and destroy all data in that file system, use the **format** command in boot loader mode.

format *filesystem***:**

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Caution Use this command with care; it destroys all data on the file system and renders your system unusable.

fsck

To check the file system for consistency, use the **fsck** command in boot loader mode.

fsck [**-test** | **-f**] *filesystem***:**

Syntax Description

-test	(Optional) Initializes the file system code and perform extra POST on flash memory. An extensive, nondestructive memory test is performed on every byte that makes up the file system.
-f	(Optional) Initializes the file system code and perform a fast file consistency check. Cyclic redundancy checks (CRCs) in the flashfs sectors are not checked.
*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.

Defaults

No file system check is performed.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

To stop an in-progress file system consistency check, disconnect the switch power and then reconnect the power.

Examples

This example shows how to perform an extensive file system check on flash memory:

```
switch: fsck -test flash:
```

help

To display the available commands, use the **help** command in boot loader mode.

help

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

You can also use the question mark (?) to display a list of available boot loader commands.

memory

To display memory heap utilization information, use the **memory** command in boot loader mode.

memory

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to display memory heap utilization information:

```
switch: memory
Text:   0x00700000 - 0x0071cf24 (0x0001cf24 bytes)
Rotext: 0x00000000 - 0x00000000 (0x00000000 bytes)
Data:   0x0071cf24 - 0x00723a0c (0x00006ae8 bytes)
Bss:    0x0072529c - 0x00746f94 (0x00021cf8 bytes)
Heap:   0x00756f98 - 0x00800000 (0x000a9068 bytes)

Bottom heap utilization is 22 percent.
Top heap utilization is 0 percent.
Total heap utilization is 22 percent.
Total bytes: 0xa9068 (692328)
Bytes used: 0x26888 (157832)
Bytes available: 0x827e0 (534496)

Alternate heap utilization is 0 percent.
Total alternate heap bytes: 0x6fd000 (7327744)
Alternate heap bytes used: 0x0 (0)
Alternate heap bytes available: 0x6fd000 (7327744)
```

Table A-2 describes the fields in the display.

Table A-2 memory Field Descriptions

Field	Description
Text	Beginning and ending address of the text storage area.
Rotext	Beginning and ending address of the read-only text storage area. This part of the data segment is grouped with the Text entry.
Data	Beginning and ending address of the data segment storage area.
Bss	Beginning and ending address of the block started by symbol (Bss) storage area. It is initialized to zero.
Heap	Beginning and ending address of the area in memory that memory is dynamically allocated to and freed from.

mgmt_clr

To clear the Ethernet management port statistics, use the **mgmt_clr** command in boot loader mode.

mgmt_clr

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to clear the Ethernet management port statistics:

```
switch: mgmt_clr
```

mgmt_init

To initialize the Ethernet management port, use the **mgmt_init** command in boot loader mode.

mgmt_init

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Use the **mgmt_init** command only during debugging of the Ethernet management port.

Examples

This example shows how to initialize the Ethernet management port:

```
switch: mgmt_init
```

mgmt_show

To display the Ethernet management port statistics, use the **mgmt_show** command in boot loader mode.

mgmt_show

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to display the Ethernet management port statistics:

```
switch: mgmt_show
Statistics                Received    Transmitted
-------------------------------------------------
good frame bytes      :          60            120
good frames           :           1              2
bad frames            :           0              0
dropped frames        :           0              0
queue overflowed      :           0              0
memory access errors  :           0              0
```

mkdir

To create one or more new directories on the specified file system, use the **mkdir** command in boot loader mode.

mkdir *filesystem***:/***directory-url ...*

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/directory-url	Name of the directories to create. Separate each directory name with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Directory names are case sensitive.

Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Examples

This example shows how to make a directory called Saved_Configs:

```
switch: mkdir flash:Saved_Configs
Directory "flash:Saved_Configs" created
```

This example shows how to make two directories:

```
switch: mkdir flash:Saved_Configs1 flash:Test
Directory "flash:Saved_Configs1" created
Directory "flash:Test" created
```

You can verify that the directory was created by entering the **dir** *filesystem***:** boot loader command.

Related Commands

Command	Description
dir	Displays a list of files and directories on the specified file system.
rmdir	Removes one or more directories from the specified file system.

more

To display the contents of one or more files, use the **more** command in boot loader mode.

more *filesystem***:/***file-url ...*

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/*file-url*	Path (directory) and name of the files to display. Separate each filename with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

Examples

This example shows how to display the contents of two files:

```
switch: more flash:/new-images/info flash:env_vars
version_suffix: image-name
version_directory: image-name
image_name: image-name.bin
ios_image_file_size: 63984644
total_image_file_size: 8133632
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
info_end:
BAUD=57600
MANUAL_BOOT=no
```

Related Commands

Command	Description
cat	Displays the contents of one or more files.
type	Displays the contents of one or more files.

peek

To read data from a memory location, use the **peek** command in boot loader mode.

peek *location*

Syntax Description

location	32-bit memory location.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to read data from a memory location:

```
switch: peek 0xfff80000
ox4BE000=102
```

ping

To send ICMP ECHO REQUEST packets to a network host, use the **ping** command in boot loader mode.

ping *ip-address*

Syntax Description

ip-address	The IP address of the network host.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to send an echo request packet to a network host:

```
switch: ping 1.1.1.1 255.255.255.0
```

poke

To write data to one writable memory location, use the **poke** command in boot loader mode.

poke *location*

Syntax Description

location	32-bit memory location.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to write data to a writeable memory location:

```
switch: poke 0xfff80000
ox4BE000=102
```

rename

To rename a file, use the **rename** command in boot loader mode.

rename *filesystem***:/***source-file-url filesystem***:/***destination-file-url*

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/*source-file-url*	Original path (directory) and filename.
/*destination-file-url*	New path (directory) and filename.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 45 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Examples

This example shows a file named *config.text* being renamed to *config1.text*:

```
switch: rename flash:config.text flash:config1.text
```

You can verify that the file was renamed by entering the **dir** *filesystem***:** boot loader command.

Related Commands

Command	Description
copy	Copies a file from a source to a destination.

reset

To perform a hard reset on the system, use the **reset** command in boot loader mode. A hard reset is similar to power-cycling the switch, clearing the processor, registers, and memory.

reset

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to reset the system:

```
switch: reset
Are you sure you want to reset the system (y/n)?y
System resetting...
```

Related Commands

Command	Description
boot	Loads and boots an executable image and enters the command-line interface.

rmdir

To remove one or more empty directories from the specified file system, use the **rmdir** command in boot loader mode.

rmdir *filesystem***:***/directory-url ...*

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/directory-url	Path (directory) and name of the empty directories to remove. Separate each directory name with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Directory names are case sensitive and limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Before removing a directory, you must first delete all the files in the directory.

The switch prompts you for confirmation before deleting each directory.

Examples

This example shows how to remove a directory:

```
switch: rmdir flash:Test
```

You can verify that the directory was deleted by entering the **dir** *filesystem***:** boot loader command.

Related Commands

Command	Description
dir	Displays a list of files and directories on the specified file system.
mkdir	Creates one or more new directories on the specified file system.

set

To set or display environmental variables that can be used to control the boot loader or any other software running on the switch, use the **set** command in boot loader mode.

set *variable value*

Note Under normal circumstances, it is not necessary to alter the setting of the environment variables.

Syntax Description

variable value	Use one of these keywords for *variable and value*:
	MANUAL_BOOT—Decides whether the switch automatically or manually boots.
	Valid values are 1, yes, 0, and no. If it is set to no or 0, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the switch from the boot loader mode.
	BOOT *filesystem***:/***file-url*—A semicolon-separated list of executable files to try to load and execute when automatically booting.
	If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash: file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system.
	ENABLE_BREAK—Decides whether the automatic boot process can be interrupted by using the Break key on the console.
	Valid values are 1, yes, on, 0, no, and off. If it is set to 1, yes, or on, you can interrupt the automatic boot process by pressing the Break key on the console after the flash file system has initialized.
	HELPER *filesystem***:/***file-url*—A semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.
	PS1 *prompt*—A string that is used as the command-line prompt in boot loader mode.
	CONFIG_FILE flash:/*file-url*—The filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
	BAUD *rate*—The rate in bits per second (bps) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting. The range is from 0 to 4294967295 bps. Valid values are 50, 75, 110, 150, 300, 600, 1200, 1800, 2000, 2400, 3600, 4800, 7200, 9600, 14400, 19200, 28800, 38400, 56000, 57600, 115200, and 128000.
	The most commonly used values are 300, 1200, 2400, 9600, 19200, 57600, and 115200.
	HELPER_CONFIG_FILE *filesystem***:/***file-url*—The name of the configuration file to be used by the Cisco IOS helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of Cisco IOS that are loaded, including the helper image. This variable is used only for internal development and testing.

Defaults

The environment variables have these default values:

MANUAL_BOOT: No (0)

BOOT: Null string

ENABLE_BREAK: No (Off or 0) (the automatic boot process cannot be interrupted by pressing the Break key on the console).

HELPER: No default value (helper files are not automatically loaded).

PS1: switch:

CONFIG_FILE: config.text

BAUD: 9600 bps

HELPER_CONFIG_FILE: No default value (no helper configuration file is specified).

SWITCH_NUMBER: 1

SWITCH_PRIORITY: 1

Note Environment variables that have values are stored in the flash file system in various files. The format of these files is that each line contains an environment variable name and an equal sign followed by the value of the variable. A variable has no value if it is not listed in this file; it has a value if it is listed in the file even if the value is a null string. A variable that is set to a null string (for example, " ") is a variable with a value. Many environment variables are predefined and have default values.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Environment variables are case sensitive and must be entered as documented.

Environment variables that have values are stored in flash memory outside of the flash file system.

Under normal circumstances, it is not necessary to alter the setting of the environmental variables.

The MANUAL_BOOT environment variable can also be set by using the **boot manual** global configuration command.

The BOOT environment variable can also be set by using the **boot system** *filesystem***:/***file-url* global configuration command.

The ENABLE_BREAK environment variable can also be set by using the **boot enable-break** global configuration command.

The HELPER environment variable can also be set by using the **boot helper** *filesystem***:/***file-url* global configuration command.

The CONFIG_FILE environment variable can also be set by using the **boot config-file flash:/***file-url* global configuration command.

The HELPER_CONFIG_FILE environment variable can also be set by using the **boot helper-config-file** *filesystem***:/***file-url* global configuration command.

The HELPER_CONFIG_FILE environment variable can also be set by using the **boot helper-config-file** *filesystem***:/***file-url* global configuration command.

The boot loader prompt string (PS1) can be up to 120 printable characters except the equal sign (=).

Examples

This example shows how to change the boot loader prompt:

```
switch: set PS1 loader:
loader:
```

You can verify your setting by using the **set** boot loader command.

Related Commands

Command	Description
unset	Resets one or more environment variables to its previous setting.

set_param

To write system parameters to the system flash memory, use the **set_param** command in boot loader mode.

set_param

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to write system parameters to system flash memory.

```
switch: set_param
```

sleep

To pause for a specified number of seconds, use the **sleep** command in boot loader mode.

sleep *value*

Syntax Description

value:	Sets the time to pause the boot loader in seconds. The range is 0 to 2^{31}–1.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to pause the boot loader process for 30 seconds:

```
switch: sleep 30
```

type

To display the contents of one or more files, use the **type** command in boot loader mode.

type *filesystem***:***/file-url ...*

Syntax Description

*filesystem***:**	Alias for a flash file system. Use **flash:** for the system board flash device.
/file-url	Path (directory) and name of the files to display. Separate each filename with a space.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

Examples

This example shows how to display the contents of two files:

```
switch: type flash:/new-images/info flash:env_vars
version_suffix: image-name
version_directory: image-name
image_name: image-name.bin
ios_image_file_size: 63984644
total_image_file_size: 8133632
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
info_end:
BAUD=57600
MANUAL_BOOT=no
```

Related Commands

Command	Description
cat	Displays the contents of one or more files.
more	Displays the contents of one or more files.

unset

To reset one or more environmental variables, use the **unset** command in boot loader mode.

unset *variable ...*

Note Under normal circumstances, it is not necessary to alter the setting of the environment variables.

Syntax Description

variable	Use one of these keywords for *variable*: **MANUAL_BOOT**—Decides whether the switch automatically or manually boots. **BOOT**—Resets the list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system. **ENABLE_BREAK**—Decides whether the automatic boot process can be interrupted by using the Break key on the console after the flash file system has been initialized. **HELPER**—A semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader. **PS1**—A string that is used as the command-line prompt in boot loader mode. **CONFIG_FILE**—Resets the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration. **BAUD**—Resets the rate in bits per second (bps) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting. **HELPER_CONFIG_FILE**—Resets the name of the configuration file to be used by the Cisco IOS helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of Cisco IOS that are loaded, including the helper image. This variable is used only for internal development and testing.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

Under normal circumstances, it is not necessary to alter the setting of the environmental variables.

The MANUAL_BOOT environment variable can also be reset by using the **no boot manual** global configuration command.

The BOOT environment variable can also be reset by using the **no boot system** global configuration command.

The ENABLE_BREAK environment variable can also be reset by using the **no boot enable-break** global configuration command.

The HELPER environment variable can also be reset by using the **no boot helper** global configuration command.

The CONFIG_FILE environment variable can also be reset by using the **no boot config-file** global configuration command.

The HELPER_CONFIG_FILE environment variable can also be reset by using the **no boot helper-config-file** global configuration command.

Examples

This example shows how to reset the prompt string to its previous setting:

```
switch: unset PS1
switch:
```

Related Commands

Command	Description
set	Sets or displays environment variables.

version

To display the boot loader version, use the **version** command in boot loader mode.

version

Syntax Description

This command has no arguments or keywords.

Command Modes

Boot loader

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Examples

This example shows how to display the boot loader version:

```
switch: version
switch-name Boot Loader (xxxxx-HBOOT-M) Version 12.2(xx)EX
Compiled Wed 12-Sept-05 14:58 by devgoyal

switch:
```

APPENDIX B

Cisco ME 3800X and ME 3600X Switch Debug Commands

This appendix describes the **debug** privileged EXEC commands that have been created or changed for use with the Cisco ME 3800X and ME 3600X switch. These commands are helpful in diagnosing and resolving internetworking problems and should be enabled only under the guidance of Cisco technical support staff.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use the **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use the **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Although visible in the command-line help, the switch does not support the **debug platform** commands.

debug bridge-domain

To enable debugging of bridge domains, use the **debug bridge-domain** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug bridge-domain {*number* **mac** {**security** | **table**} {**errors** | **events**} | **configuration** | **errors** | **ipc**}

no debug bridge-domain {*number* **mac** {**security** | **table**} {**errors** | **events**} | **configuration** | **errors** | **ipc**}

Syntax Description

number	Enter the bridge domain number to debug. The range is 1 to 8000.
mac security	Displays MAC security debug messages.
mac table	Displays MAC address table debug messages.
errors	Displays MAC security or MAC address table error debug messages.
events	Displays MAC security or MAC address table event debug messages.
configuration	Displays bridge domain configuration event debug messages.
errors	Displays bridge domain error debug messages.
ipc	Displays bridge domain IPC error and event debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug bridge-domain** command is the same as the **no debug bridge-domain** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug etherchannel

To enable debugging of the EtherChannel/PAgP shim, use the **debug etherchannel** command in privileged EXEC mode. This shim is the software module that is the interface between the Port Aggregation Protocol (PAgP) software module and the port manager software module. To disable debugging, use the **no** form of this command.

debug etherchannel [**all** | **detail** | **error** | **event** | **idb**]

no debug etherchannel [**all** | **detail** | **error** | **event** | **idb**]

Syntax Description

all	(Optional) Displays all EtherChannel debug messages.
detail	(Optional) Displays detailed EtherChannel debug messages.
error	(Optional) Displays EtherChannel error debug messages.
event	(Optional) Displays major EtherChannel event messages.
idb	(Optional) Displays PAgP interface descriptor block debug messages.

Note Though visible in the command-line help strings, the **linecard** keyword is not supported.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If you do not specify a keyword, all debug messages appear.

The **undebug etherchannel** command is the same as the **no debug etherchannel** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show etherchannel	Displays EtherChannel information for the channel.

debug ethernet service

To enable debugging of Ethernet customer service instances, use the **debug ethernet service** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug ethernet service {**all** | **api** | **error** | **evc** [**id** *evc-id*] | **instance** [**id** *id interface-id* | **interface** *interface-id*] | **interface** [*interface-id*] | **oam-mgr**}

no debug ethernet service {**all** | **api** | **error** | **evc [id** *evc-id*] | **instance** [**id** *id interface-id* | **interface** *interface-id*] | **interface** [*interface-id*] | **oam-mgr**}

Syntax Description

all	Displays all Ethernet customer-service debug messages.
api	Displays debug messages about the interaction between the Ethernet infrastructure and its clients.
error	Displays Ethernet customer-service error messages occurring in the Ethernet infrastructure subsystem.
evc	Displays Ethernet virtual connection (EVC) debug messages
id *evc-id*	(Optional) Displays EVC debug messages relevant to a specific EVC identifier. The EVC identifier can be a string of from 1 to 100 characters.
instance	Displays debug messages related to Ethernet customer-service instances.
id *id interface-id*	(Optional) Displays Ethernet service-instance debug messages for a specific Ethernet service instance ID and interface. The service identifier range is 1 to 4294967295. The interface is a physical interface.
interface *interface-id*	(Optional) When entered after the **instance** keyword, displays service-instance debug messages for the interface. You must enter an interface ID.
interface [*interface-id*]	Displays debugging for Ethernet services on all interfaces or the specified interface.
oam-mgr	Displays debug messages for the Ethernet operation, administration, and maintenance (OAM) manager component of the infrastructure.

Command Default

Ethernet service debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug ethernet service** command is the same as the **no debug ethernet service** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug interface

To enable debugging of interface-related activities, use the **debug interface** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug interface {*interface-id* | **null** *interface-number* | **port-channel** *port-channel-number* | **vlan** *vlan-id*}

no debug interface {*interface-id* | **null** *interface-number* | **port-channel** *port-channel-number* | **vlan** *vlan-id*}

Syntax Description

interface-id	Displays debug messages for the specified physical port, identified by type switch number/module number/ port, for example **gigabitethernet 0/2**.
null *interface-number*	Displays debug messages for null interfaces. The *interface-number* is always **0**.
port-channel *port-channel-number*	Displays debug messages for the specified EtherChannel port-channel interface. The *port-channel-number* range is 1 to 26.
vlan *vlan-id*	Displays debug messages for the specified VLAN. The *vlan-id* range is 1 to 4094.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

If you do not specify a keyword, all debug messages appear.

The **undebug interface** command is the same as the **no debug interface** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show interface	Displays interface status and configuration information.

debug ip igmp filter

To enable debugging of Internet Group Management Protocol (IGMP) filter events, use the **debug ip igmp filter** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug ip igmp filter

no debug ip igmp filter

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug ip igmp filter** command is the same as the **no debug ip igmp filter** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug ip igmp max-groups

To enable debugging of Internet Group Management Protocol (IGMP) maximum groups events, use the **debug ip igmp max-groups** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug ip igmp max-groups

no debug ip igmp max-groups

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug ip igmp max-groups** command is the same as the **no debug ip igmp max-groups** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug ip igmp snooping

To enable debugging of Internet Group Management Protocol (IGMP) snooping activity, use the **debug igmp snooping** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug ip igmp snooping [*ip_address* | **group** | **management** | **querier** | **redundancy** | **router** | **timer**]

no debug ip igmp snooping [*ip_address* | **group** | **management** | **querier** | **redundancy** | **router** | **timer**]

Syntax Description

ip_address	IPv4 group address
group	(Optional) Displays IGMP snooping group activity debug messages.
management	(Optional) Displays IGMP snooping management activity debug messages.
querier	(Optional) Displays IGMP snooping querier debug messages.
redundancy	(Optional) Displays IGMP snooping redundancy events.
router	(Optional) Displays IGMP snooping router activity debug messages.
timer	(Optional) Displays IGMP snooping timer event debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug ip igmp snooping** command is the same as the **no debug ip igmp snooping** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug lacp

To enable debugging of Link Aggregation Control Protocol (LACP) activity, use the **debug lacp** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug lacp [**all** | **event** | **fsm** | **misc** | **packet**]

no debug lacp [**all** | **event** | **fsm** | **misc** | **packet**]

Syntax Description

all	(Optional) Displays all LACP debug messages.
event	(Optional) Displays LACP event debug messages.
fsm	(Optional) Displays LACP finite state-machine debug messages.
misc	(Optional) Displays miscellaneous LACP debug messages.
packet	(Optional) Displays LACP packet debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug lacp** command is the same as the **no debug lacp** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show lacp	Displays LACP channel-group information.

debug mac-notification

To enable debugging of MAC notification events, use the **debug mac-notification** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug mac-notification

no debug mac-notification

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug mac-notification** command is the same as the **no debug mac-notification** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show mac address-table notification	Displays the MAC address notification information for all interfaces or the specified interface.

debug matm

To enable debugging of platform-independent MAC address management events, use the **debug matm** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug matm {**add** | **age** | **all** | **bulkdelete** | **create** | **delete** | **error** | **move** | **pm** | **remove** | **traceback**}

no debug matm {**add** | **age** | **all** | **bulkdelete** | **create** | **delete** | **error** | **move** | **pm** | **remove** | **traceback**}

Syntax Description

add	Displays MAC address add debug messages.
age	Displays MAC address aging debug messages.
all	Displays all MAC address debug messages.
bulkdelete	Displays MAC address bulk delete debug messages.
create	Displays MAC address creation debug messages.
delete	Displays MAC address deletion debug messages.
error	Displays MAC address creation debug messages.
move	Displays MAC address move debug messages.
pm	Displays MAC address port manager debug messages.
remove	Displays MAC address remove debug messages.
traceback	Displays MAC address traceback debug messages.

Note Although visible in the command-line help, the **pvlan** keyword is not supported.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug matm** command is the same as the **no debug matm** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug matm move

To enable debugging of MAC address-table move message processing, use the **debug matm move** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug matm move [**address | update**]

no debug matm move [**address | update**]

Syntax Description

address	Displays MAC address table move address debug messages.
move	Displays MAC address table move update debug messages.

Defaults

Debugging is disabled. update

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug matm move** command is the same as the **no debug matm move** command.

Related Commands

Command	Description
mac address-table move update	Configures the MAC address-table move update feature on the switch.
show debugging	Displays information about the types of debugging that are enabled.
show mac address-table move update	Displays the MAC address-table move update information on the switch.

debug network-clock

To enable debugging of a SyncE network clock, use the **debug network-clock** command in Privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug network-clock [**error**] [**event**] [**pal**] [**sm**]

no debug network-clock [**error**] [**event**] [**pal**] [**sm**]

Syntax Description

error	Network clock error debugging
event	Network clock event debugging
pal	Network clock PAL debugging
sm	Network clock state machine debugging

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(2)EY	This command was introduced.

Usage Guidelines

Examples

The following example shows how to enable SyncE network clock debugging:

```
Switch# deb network-clock ?
  error  Network clock error debugging
  event  Network clock event debugging
  pal    Network clock PAL debugging
  sm     Network clock state machine debugging

Switch# deb network-clock error
```

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug nvram

To enable debugging of NVRAM activity, use the **debug nvram** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug nvram

no debug nvram

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug nvram** command is the same as the **no debug nvram** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug pagp

To enable debugging of Port Aggregation Protocol (PAgP) activity, use the **debug pagp** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug pagp [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

no debug pagp [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

Syntax Description

all	(Optional) Displays all PAgP debug messages.
dual-active	(Optional) Displays PAgP dual-active debug messages.
event	(Optional) Displays PAgP event debug messages.
fsm	(Optional) Displays PAgP finite state-machine debug messages.
misc	(Optional) Displays miscellaneous PAgP debug messages.
packet	(Optional) Displays PAgP packet debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug pagp** command is the same as the **no debug pagp** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show pagp	Displays PAgP channel-group information.

debug pm

To enable debugging of port manager (PM) activity, use the **debug pm** command in privileged EXEC mode. The port manager is a state machine that controls all the logical and physical interfaces. All features, such as VLANs, UniDirectional Link Detection (UDLD), and so forth, work with the port manager to provide switch functions. To disable debugging, use the **no** form of this command.

debug pm {**all** | **assert** | **card** | **cookies** | **etherchnl** | **hatable** | **messages** | **port** | **redundancy** | **registry** | **sm** | **span** | **split** | **statistics**| **vlan** | **vp**}

no debug pm {**all** | **assert** | **card** | **cookies** | **etherchnl** | **hatable** | **messages** | **port** | **redundancy** | **registry** | **sm** | **span** | **split** | **statistics**| **vlan** | **vp**}

Syntax Description

all	Displays all PM debug messages.
assert	Displays assert debug messages.
card	Displays line-card related-events debug messages.
cookies	Displays internal PM cookie validation debug messages.
etherchnl	Displays EtherChannel related-events debug messages.
hatable	Displays Host Access Table events debug messages.
messages	Displays PM debug messages.
port	Displays port related-events debug messages.
redundancy	Displays PM redundancy event debug messages.
registry	Displays PM registry invocation debug messages.
sm	Displays state-machine related-events debug messages.
span	Displays spanning-tree related-events debug messages.
split	Displays split-processor debug messages.
statistics	Displays PM statistic event debug messages.
vlan	Displays VLAN related-events debug messages.
vp	Displays virtual port related-events debug messages.

Note Though visible in the command-line help strings, the **pvlan** and **scp** keywords are not supported.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug pm** command is the same as the **no debug pm** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug rep

To enable debugging of Resilient Ethernet Protocol (REP) functions, use the **debug rep** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug rep {**all** | **bpa-event** | **bpasm** | **database** | **epa-pkt** | **epasm** | **error** | **failure-recovery** | **lslsm** | **misc** | **packet** | **prsm** |**show cli**}

no debug rep {**all** | **bpa-event** | **bpasm** | **database** | **epa-pkt** | **epasm** | **error** | **failure-recovery** | **lslsm** | **misc** | **packet** | **prsm** |**show cli**}

Syntax Description

all	Display all REP debug messages.
bpa-event	Displays blocked port advertisement (BPA) debug messages.
bpasm	Displays BPA state machine debug messages.
database	Displays REP state machine debug messages.
epa-pkt	Displays end port advertisement (EPA) packet debug messages.
epasm	Displays EPA state machine debug messages.
error	Displays REP protocol error debug messages.
failure-recovery	Displays REP switchover event debug messages.
lslsm	Displays Link State Layer (LSL) state machine debug messages.
misc	Displays miscellaneous REP debug messages.
packet	Displays protocol PDU debug messages.
prsm	Displays REP port role state machine debug messages.
showcli	Displays show command line interface debug information.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug rep** command is the same as the **no debug rep** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show interfaces rep	Displays REP configuration and status for a specified interface or for all interfaces.

debug qos

To enable debugging of the quality of service (QoS) feature, use the **debug qos** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug qos {**capability** | **events** | **service-policy** {**global-lock** | **iteration** | **lifecycle** | **polling** | **stats trace**} | **set**}

no debug qos {**capability** | **events** | **service-policy** {**global-lock** | **iteration** | **lifecycle** | **polling** | **stats trace**} | **set**}

Syntax Description

capability	Displays all QoS capability debug messages.
events	Displays modular QoS command-line interface (MQC) event debug messages.
service-policy	Displays QoS service policy debug messages.
global-lock	Displays QoS service policy lock event debug messages.
iteration	Displays QoS service policy iteration debug messages.
lifecycle	Displays QoS service policy install and remove event debug messages.
polling	Displays QoS service policy statistics polling debug messages.
stats	Displays QoS service policy statistics update debug messages.
trace	Includes traceback information in the debug message output.
set	Displays QoS packet marking debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug qos** command is the same as the **no debug qos** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug spanning-tree

To enable debugging of spanning-tree activities, use the **debug spanning-tree** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree {**all** | **bpdu** | **bpdu-opt** | **config** | **etherchannel** | **events** | **exceptions** | **general** | **mstp** | **pvst+** | **root** | **snmp** | **switch** | **synchronization** | **vlan-shim**}

no debug spanning-tree {**all** | **bpdu** | **bpdu-opt** | **config** | **etherchannel** | **events** | **exceptions** | **general** | **mstp** | **pvst+** | **root** | **snmp** | **switch** | **synchronization** | **vlan-shim**}

Syntax Description

all	Displays all spanning-tree debug messages.
bpdu	Displays spanning-tree bridge protocol data unit (BPDU) debug messages. See the **debug spanning-tree bpdu** command.
bpdu-opt	Displays optimized BPDU handling debug messages. See the **debug spanning-tree bpdu-opt** command.
config	Displays spanning-tree configuration change debug messages.
etherchannel	Displays EtherChannel-support debug messages.
events	Displays spanning-tree topology event debug messages.
exceptions	Displays spanning-tree exception debug messages.
general	Displays general spanning-tree activity debug messages.
mstp	Debug Multiple Spanning Tree Protocol events. See the **debug spanning-tree mstp** command.
pvst+	Displays per-VLAN spanning-tree plus (PVST+) event debug messages.
root	Displays spanning-tree root-event debug messages.
snmp	Displays spanning-tree Simple Network Management Protocol (SNMP) handling debug messages.
switch	Displays switch shim command debug messages. This shim is the software module that is the interface between the generic Spanning Tree Protocol (STP) code and the platform-specific code of various switch platforms. See the **debug spanning-tree switch** command.
synchronization	Displays the spanning-tree synchronization event debug messages.
vlan-shim	Displays spanning-tree VLAN shim debug messages. See the **debug spanning-tree vlan-shim** command

Note Though visible in the command-line help strings, the **csuf/csrt** keyword is not supported.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug spanning-tree command is the** same as the **no debug spanning-tree** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show spanning-tree	Displays spanning-tree state information.

debug spanning-tree bpdu

To enable debugging of sent and received spanning-tree bridge protocol data units (BPDUs), use the **debug spanning-tree bpdu** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree bpdu [**receive | transmit**]

no debug spanning-tree bpdu [**receive | transmit**]

Syntax Description

receive	(Optional) Displays the nonoptimized path for received BPDU debug messages.
transmit	(Optional) Displays the nonoptimized path for sent BPDU debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug spanning-tree bpdu** command is the same as the **no debug spanning-tree bpdu** command**.**

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show spanning-tree	Displays spanning-tree state information.

debug spanning-tree bpdu-opt

To enable debugging of optimized spanning-tree bridge protocol data units (BPDUs) handling, use the **debug spanning-tree bpdu-opt** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree bpdu-opt [**detail | packet**]

no debug spanning-tree bpdu-opt [**detail | packet**]

Syntax Description

detail	(Optional) Displays detailed optimized BPDU-handling debug messages.
packet	(Optional) Displays packet-level optimized BPDU-handling debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug spanning-tree bpdu-opt** command is the same as the **no debug spanning-tree bpdu-opt** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show spanning-tree	Displays spanning-tree state information.

debug spanning-tree mstp

To enable debugging of the Multiple Spanning Tree Protocol (MSTP) feature, use the **debug spanning-tree mstp** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree mstp {**all** | **boundary** | **bpdu-rx** | **bpdu-tx** | **errors** | **flush** | **init** | **migration** | **pm** | **proposals** | **region** | **roles** | **sanity_check** | **sync** | **tc** | **timers**}

no debug spanning-tree mstp {**all** | **boundary** | **bpdu-rx** | **bpdu-tx** | **errors** | **flush** | **init** | **migration** | **pm** | **proposals** | **region** | **roles** | **sanity_check** | **sync** | **tc** | **timers**}

Syntax Description

all	Enables all the debugging messages.
boundary	Displays flag changes at these boundaries: • An multiple spanning-tree (MST) region and a single spanning-tree region running Rapid Spanning Tree Protocol (RSTP) • An MST region and a single spanning-tree region running IEEE 802.1D • An MST region and another MST region with a different configuration
bpdu-rx	Displays the received MST bridge protocol data units (BPDUs).
bpdu-tx	Displays the sent MST BPDUs.
errors	Displays MSTP errors.
flush	Displays the port flushing mechanism.
init	Displays the initialization of the MSTP data structures.
migration	Debug the protocol migration state machine.
pm	Displays MSTP port manager events.
proposals	Displays handshake messages between the designated switch and the root switch.
region	Displays the region synchronization between the switch processor (SP) and the route processor (RP).
roles	Displays MSTP roles.
sanity_check	Displays the received BPDU sanity check messages.
sync	Displays the port synchronization events.
tc	Displays topology change notification events.
timers	Displays the MSTP timers for start, stop, and expire events.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug spanning-tree mstp** command is the same as the **no debug spanning-tree mstp** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show spanning-tree	Displays spanning-tree state information.

debug spanning-tree switch

To enable debugging of the software interface between the Spanning Tree Protocol (STP) and the port manager, use the **debug spanning-tree switch** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree switch {**all** | **errors** | **flush** | **general** | **helper** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** [**decode**]}

no debug spanning-tree switch {**all** | **errors** | **flush** | **general** | **helper** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** [**decode**]}

Syntax Description

all	Displays all spanning-tree switch debug messages.
errors	Displays debug messages for the interface between the spanning-tree software module and the port manager software module.
flush	Displays debug messages for the shim flush operation.
general	Displays general event debug messages.
helper	Displays spanning-tree helper-task debug messages. Helper tasks handle bulk spanning-tree updates.
pm	Displays port-manager event debug messages.
rx	Displays received bridge protocol data unit (BPDU) handling debug messages. The keywords have these meanings: • **decode**—Display decoded received packets. • **errors**—Display receive error debug messages. • **interrupt**—Display interrupt service request (ISR) debug messages. • **process**—Display process receive BPDU debug messages.
state	Displays spanning-tree port state change debug messages;
tx [**decode**]	Displays sent BPDU handling debug messages. The keyword has this meaning: • **decode**—(Optional) Display decoded sent packets.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug spanning-tree switch** command is the same as the **no debug spanning-tree switch** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show spanning-tree	Displays spanning-tree state information.

debug spanning-tree vlan-shim

To enable debugging of the Spanning Tree Protocol (STP) VLAN shim, use the **debug spanning-tree switch** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree vlan-shim {**all** | **errors** | **flush** | **general** | **helper** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** [**decode**]}

no debug spanning-tree vlan-shim {**all** | **errors** | **flush** | **general** | **helper** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** [**decode**]}

Syntax Description

all	Displays all spanning-tree VLAN debug messages.
errors	Displays debug messages for STP VLAN errors.
flush	Displays debug messages for the VLAN shim flush operation.
general	Displays general VLAN event debug messages.
helper	Displays spanning-tree helper-task debug messages. Helper tasks handle bulk spanning-tree updates.
rx	Displays received bridge protocol data unit (BPDU) handling debug messages. The keywords have these meanings: • **decode**—Displays decoded received packets. • **errors**—Displays receive error debug messages. • **interrupt**—Displays interrupt service request (ISR) debug messages. • **process**—Displays process receive BPDU debug messages.
state	Displays spanning-tree port state change debug messages;
tx [**decode**]	Displays sent BPDU handling debug messages. The keyword has this meaning: • **decode**—(Optional) Display decoded sent packets.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug spanning-tree vlan-shim** command is the same as the **no debug spanning-tree vlan-shim** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show spanning-tree	Displays spanning-tree state information.

debug sw-vlan

To enable debugging of VLAN manager activities, use the **debug sw-vlan** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan {**badpmcookies** | **cfg-vlan** {**bootup** | **cli**} | **events** | **ifs** | **management** | **notification** | **packets** | **registries**}

no debug sw-vlan {**badpmcookies** | **cfg-vlan** {**bootup** | **cli**} | **events** | **ifs** | **management** | **notification** | **packets** | **registries**}

Syntax Description

badpmcookies	Displays debug messages for VLAN manager incidents of bad port manager cookies.
cfg-vlan {**bootup** | **cli**}	Displays config-vlan debug messages. The keywords have these meanings: • **bootup**—Display messages when the switch is booting up. • **cli**—Display messages when the command-line interface (CLI) is in config-vlan mode.
events	Displays debug messages for VLAN manager events.
ifs	See the **debug sw-vlan ifs** command.
management	Displays debug messages for VLAN manager management of internal VLANs.
notification	See the **debug sw-vlan notification** command.
packets	Displays debug messages for packet handling and encapsulation processes.
registries	Displays debug messages for VLAN manager registries.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug sw-vlan** command is the same as the **no debug sw-vlan** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.

debug sw-vlan ifs

To enable debugging of the VLAN manager IOS file system (IFS) error tests, use the **debug sw-vlan ifs** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan ifs {**open** {**read** | **write**} | **read** {**1** | **2** | **3** | **4**} | **write**}

no debug sw-vlan ifs {**open** {**read** | **write**} | **read** {**1** | **2** | **3** | **4**} | **write**}

Syntax Description

open {**read** | **write**}	Displays VLAN manager IFS file-open operation debug messages. The keywords have these meanings: • **read**—Display VLAN manager IFS file-read operation debug messages. • **write**—Display VLAN manager IFS file-write operation debug messages.
read {**1** | **2** | **3** | **4**}	Displays file-read operation debug messages for the specified error test (1, 2, 3, or 4).
write	Displays file-write operation debug messages.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug sw-vlan ifs** command is the same as the **no debug sw-vlan ifs** command.

When selecting the file read operation, Operation **1** reads the file header, which contains the header verification word and the file version number. Operation **2** reads the main body of the file, which contains most of the domain and VLAN information. Operation **3** reads type length version (TLV) descriptor structures. Operation **4** reads TLV data.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.

debug sw-vlan notification

To enable debugging of the activation and deactivation of VLAN IDs, use the **debug sw-vlan notification** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan notification {**accfwdchange** | **allowedvlancfgchange** | **fwdchange** | **linkchange** | **modechange** | **statechange**}

no debug sw-vlan notification {**accfwdchange** | **allowedvlancfgchange** | **fwdchange** | **linkchange** | **modechange** | **statechange**}

Syntax Description

accfwdchange	Displays debug messages for VLAN manager notification of aggregated access interface spanning-tree forward changes.
allowedvlancfgchange	Displays debug messages for VLAN manager notification of changes to the allowed VLAN configuration.
fwdchange	Displays debug messages for VLAN manager notification of spanning-tree forwarding changes.
linkchange	Displays debug messages for VLAN manager notification of interface link-state changes.
modechange	Displays debug messages for VLAN manager notification of interface mode changes.
statechange	Displays debug messages for VLAN manager notification of interface state changes.

Note Though visible in the command-line help strings, the **pruningcfgchange** keyword is not supported.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug sw-vlan notification** command is the same as the **no debug sw-vlan notification** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show vlan	Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain.

debug udld

To enable debugging of the UniDirectional Link Detection (UDLD) feature, use the **debug udld** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug udld {**events** | **packets** | **registries**}

no debug udld {**events** | **packets** | **registries**}

Syntax Description

events	Displays debug messages for UDLD process events as they occur.
packets	Displays debug messages for the UDLD process as it receives packets from the packet queue and tries to send them at the request of the UDLD protocol code.
registries	Displays debug messages for the UDLD process as it processes registry calls from the UDLD process-dependent module and other feature modules.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug udld** command is the same as the **no debug udld** command.

For **debug udld events**, these debugging messages appear:

- General UDLD program logic flow
- State machine state changes
- Program actions for the set and clear ErrDisable state
- Neighbor cache additions and deletions
- Processing of configuration commands
- Processing of link-up and link-down indications

For **debug udld packets**, these debugging messages appear:

- General packet processing program flow on receipt of an incoming packet
- Indications of the contents of the various pieces of packets received (such as type length versions [TLVs]) as they are examined by the packet reception code
- Packet transmission attempts and the outcome

For **debug udld registries**, these categories of debugging messages appear:

- Sub-block creation
- Fiber-port status changes

- State change indications from the port manager software
- MAC address registry calls

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show udld	Displays UDLD administrative and operational status for all ports or the specified port.

debug vfi

To enable debugging of the virtual forwarding infrastructure (VFI) feature, use the **debug vfi** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug vfi [**fsm**] {**error** | **event**}

no debug vfi [**fsm**] {**error** | **event**}

Syntax Description

fsm	(Optional) Displays VFI finite state-machine debug messages.
error	Displays debug messages for VFI errors or VFI finite state-machine errors.
events	Displays debug messages for VFI events or VFI finite state-machine events as they occur.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug vfi** command is the same as the **no debug vfi** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
show vfi	Displays VFI status for the switch.

debug vrrp

To enable debugging of the Virtual Router Redundancy Protocol (VRRP), use the **debug vrrp** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug vrrp {**all** | **errors** | **events** | **packets** | **process** | **registry** | **state** | **timer** | **track**}

no debug vrrp {**all** | **errors** | **events** | **packets** | **process** | **registry** | **state** | **timer** | **track**}

Syntax Description

all	Displays all VRRP debug messages.
errors	Displays debug messages for VRRP error reporting.
events	Displays debug messages for protocol and interface events.
packets	Displays debug messages. for VRRP packet details.
process	Displays debug messages for VRRP process activities.
registry	Displays debug messages for VRRP registry reporting.
state	Displays VRRP state change debug messages;
timer	Displays debug messages for VRRP timer reporting.
track	Displays debug messages VRRP monitor tracking.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug vrrp** command is the same as the **no debug vrrp** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.

debug xconnect

to enable debugging of the xconnect virtual connection or virtual connection infrastructure (VFI), use the **debug xconnect** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug xconnect {**error** | **event**}

no debug xconnect {**error** | **event**}

Syntax Description

error	Displays debug messages for xconnect authorization errors.
events	Displays debug messages for xconnect authorization events.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(52)EY	This command was introduced.

Usage Guidelines

The **undebug xconnect** command is the same as the **no debug xconnect** command.

Related Commands

Command	Description
show debugging	Displays information about the types of debugging that are enabled.
xconnect	Enable xconnect on an interface.

APPENDIX C

Acknowledgments for Open-Source Software

The Cisco IOS software pipe command uses Henry Spencer's regular expression library (regex). The most recent version of the library has been modified slightly in the Catalyst operating system software to maintain compatibility with earlier versions of the library.

Henry Spencer's regular expression library (regex). Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

Permission is granted to anyone to use this software for any purpose on any computer system, and to alter it and redistribute it, subject to the following restrictions:

1. The author is not responsible for the consequences of use of this software, no matter how awful, even if they arise from flaws in it.
2. The origin of this software must not be misrepresented, either by explicit claim or by omission. Since few users ever read sources, credits must appear in the documentation.
3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software. Since few users ever read sources, credits must appear in the documentation.
4. This notice may not be removed or altered.

INDEX

A

access control entries
  See ACEs
access control lists
  See ACLs
access groups
  IP 2-94
  MAC, displaying 3-101
  matching for QoS classification 2-162, 2-165
access mode 4-69
access ports 4-69
ACEs 2-55, 2-203
ACLs
  as match criteria for QoS classes 2-162
  deny 2-53
  displaying 3-26
  for non-IP protocols 2-142
  IP 2-95
  on Layer 2 interfaces 2-95
  permit 2-201
action command 2-1
aggregate-port learner 2-197
alarm-contact command 2-5
alarm-contact status, displaying 3-49
allowed VLANs 4-71
archive download-sw command 2-7
archive tar command 2-10
archive upload-sw command 2-13
arp (boot loader) command A-2
attaching policy maps to interfaces 3-6
autonegotiation of duplex mode 2-63

B

backup interfaces, configuring 4-62
bandwidth command 2-15
BITS clock controller 2-47
BITS clock output 2-45
boot (boot loader) command A-3
boot config-file command 2-18
boot helper command 2-19
boot helper-config file command 2-20
booting
  Cisco IOS image 2-23
  displaying environment variables 3-30
  manually 2-21
boot loader
  accessing A-1
  booting
    Cisco IOS image A-3
    helper image 2-19
  directories
    creating A-18
    displaying a list of A-8
    removing A-25
  displaying
    available commands A-13
    memory heap utilization A-14
    version A-34
  environment variables
    described A-26
    displaying settings A-26
    location of A-27
    setting A-26
    unsetting A-32

files
copying A-6
deleting A-7
displaying a list of A-8
displaying the contents of A-5, A-19, A-31
renaming A-23
file system
formatting A-11
initializing flash A-10
running a consistency check A-12
prompt A-1
resetting the system A-24
boot manual command 2-21
boot private-config-file command 2-22
boot system command 2-23
BPDU filtering, for spanning tree 4-46
BPDU guard, for spanning tree 4-16, 4-46
bridge domains, displaying the MAC address table 3-109
broadcast storm control 4-55
burst bytes, in QoS policers 2-204

C

cat (boot loader) command A-5
CBWFQ, configuring 2-15
CFM 2-196
CFM as OAM protocol 2-196
channel-group command 2-24
channel-protocol command 2-27
class-based traffic shaping 3-24
class-based weighted fair queuing
See CBWFQ
class command 2-28
classification, per-port per VLAN 2-174
class-map command 2-30
class-map configuration mode 2-30
class maps
creating 2-30
defining the match criteria 2-163
displaying 3-34
matching in 2-30
class of service
See CoS
clear ipc command 2-32
clear lacp command 2-33
clear logging onboard command 2-34
clear mac address-table command 2-35
clear pagp command 2-37, 2-38
clear spanning-tree counters command 2-39
command modes defined 1-1
committed information rate in QoS policers 2-204
configuration files
password recovery disable considerations A-1
specifying the name 2-18, 2-22
configuring multiple interfaces 2-90
conform-action command 2-41
controller BITS input applique command 2-43
controller BITS output applique command 2-45
controller BITS shutdown command 2-47
copy (boot loader) command A-6
copy logging onboard module command 2-48
CoS
as match criteria for QoS groups 2-163
for QoS classification 3-8
setting value in policy maps 3-8
CPU ASIC statistics, displaying 3-36
cpu traffic qos qos-group command 2-50

D

debug bridge-domain command B-2
debug etherchannel command B-3
debug ethernet service command B-4
debug interface command B-6
debug ip igmp filter command B-7
debug ip igmp max-groups command B-8
debug ip igmp snooping command B-9
debug lacp command B-10

debug mac-notification command B-11
debug matm command B-12
debug matm move update command B-13
debug network-clock command B-14
debug nvram command B-15
debug pagp command B-16
debug pm command B-17
debug qos command B-20
debug rep command B-19
debug spanning-tree bpdu command B-23
debug spanning-tree bpdu-opt command B-24
debug spanning-tree command B-21
debug spanning-tree mstp command B-25
debug spanning-tree switch command B-27, B-29
debug sw-vlan command B-31
debug sw-vlan ifs command B-32
debug sw-vlan notification command B-33
debug udld command B-35
debug vfi command B-37
debug vrrp command B-38
debug xconnect command B-39
define interface-range command 2-50
delete (boot loader) command A-7
delete command 2-52
deny command 2-53
detect mechanism, causes 2-64
diagnostic schedule test command 2-56
diagnostic start test command 2-58
differentiated service code point
  See DSCP
Digital Optical Monitoring
  see DoM
dir (boot loader) command A-8
directories, deleting 2-52
DoM
  displaying supported transceivers 3-76
  enabling traps for 4-6
  transceivers traps 4-7
domains, CFM 2-196
dropping packets, with ACL matches 2-1
DSCP
  as match criteria for QoS groups 2-166, 2-170, 2-174
  for QoS traffic marking 3-11
  setting in policy maps 3-11
duplex command 2-62

E

E-LMI, enabling 2-70
environment variables, displaying 3-30
EoMPLS, configuring 4-98
errdisable detect cause command 2-64
errdisable recovery command 2-66
error conditions, displaying 3-54
error disable detection 2-64
error-disabled interfaces, displaying 3-64
EtherChannel
  creating port-channel logical interface 2-88
  debug EtherChannel/PAgP, display B-3
  displaying 3-58
  interface information, displaying 3-64
  LACP
    debug messages, display B-10
    displaying 3-90
    modes 2-24
    port priority for hot-standby ports 2-129
    system priority 2-131
  load-distribution methods 2-211
  PAgP
    aggregate-port learner 2-197
    clearing channel-group information 2-37
    debug messages, display B-16
    displaying 3-128
    error detection for 2-64
    error recovery timer 2-66
    learn method 2-197
    modes 2-24
    physical-port learner 2-197

Ethernet controller, internal register display 3-38
ethernet evc command 2-69
ethernet lmi ce-vlan map command 2-70
ethernet lmi command 2-70
ethernet lmi global command 2-70
Ethernet Local Management Interface
See E-LMI
ethernet oam remote-failure command 2-72
Ethernet service
debugging B-4
displaying 3-61
Ethernet service instance 3-2
Ethernet statistics, collecting 3-1
ethernet uni id command 2-73
Ethernet virtual connections
See EVCs
EVC configuration mode 2-69
EVCs
creating 2-69
service instances 3-2
UNI counts 4-85
EVC service
point-to-multipoint 4-85
point-to-point 4-85
exceed-action command 2-78
exit command, VFI configuration mode 2-127
extended-range VLANs
and allowed VLAN list 4-71
configuring 4-90
extended system ID for STP 4-22
external alarms, configuring 2-5

F

failure logging data
clearing 2-34
copying 2-48
fan information, displaying 3-49
files, deleting 2-52
flash_init (boot loader) command A-10
Flex Links
configuring 4-62
configuring preferred VLAN 4-64
flowcontrol command 2-80
format (boot loader) command A-11
forwarding packets, with ACL matches 2-1
fsck (boot loader) command A-12

G

global configuration mode 1-2, 1-3

H

hardware ACL statistics 3-26
help (boot loader) command A-13
hierarchical virtual private LAN service
See H-VPLS
host connection, port configuration 4-68
H-VPLS 2-127
configuring 2-127
displaying 3-152
hw-module module logging onboard command 2-86

I

IEEE 802.1ag Connectivity Fault Management
See CFM
IEEE 802.1Q trunk ports and native VLANs 4-95
IGMP filters
applying 2-99
debug messages, display B-7
IGMP groups, setting maximum 2-100
IGMP maximum groups, debugging B-8
IGMP profiles
creating 2-102
displaying 3-80

IGMP snooping
adding ports as a static member of a group 2-114
displaying 3-81, 3-85
enabling 2-104
enabling the configurable-leave timer 2-105
enabling the Immediate-Leave feature 2-111
flooding query count 2-109
interface topology change notification behavior 2-110
multicast table 3-83
query solicitation 2-109
report suppression 2-107
switch topology change notification behavior 2-109
images
See software images
immediate-leave processing 2-111
input policy maps
and ACL classification 2-162
commands not supported in 2-209
configuration guidelines 2-209
interface configuration mode 1-2, 1-4
interface port-channel command 2-88
interface range command 2-90
interface-range macros 2-50
interfaces
configuring 2-62
configuring multiple 2-90
creating port-channel logical 2-88
debug messages, display B-6
disabling 4-1
displaying the MAC address table 3-115
restarting 4-1
interface speed, configuring 4-53
interface vlan command 2-92
internal registers, displaying 3-38
Internet Group Management Protocol
See IGMP
invalid GBIC
error detection for 2-64
error recovery timer 2-66
ip address command 2-97
IP addresses, setting 2-97
IP address matching 2-160
ip igmp filter command 2-99
ip igmp max-groups command 2-100
ip igmp profile command 2-102
ip igmp snooping command 2-104
ip igmp snooping last-member-query-interval command 2-105
ip igmp snooping report-suppression command 2-107
ip igmp snooping tcn command 2-109
ip igmp snooping tcn flood command 2-110
ip igmp snooping vlan immediate-leave command 2-111
ip igmp snooping vlan mrouter command 2-112
ip igmp snooping vlan static command 2-114
IP precedence, as match criteria for QoS groups 2-168
ip ssh command 2-124

L

l2protocol command 2-125
l2 vfi command 2-127
lacp port-priority command 2-129
lacp system-priority command 2-131
Layer 2 mode, enabling 4-58
Layer 2 traceroute
IP addresses 4-78
MAC addresses 4-75
Layer 3 mode, enabling 4-58
line configuration mode 1-2, 1-4
link flap
error detection for 2-64
error recovery timer 2-66
load-distribution methods for EtherChannel 2-211
location (global configuration) command 2-133
location (interface configuration) command 2-135
logging event command 2-137
logging file command 2-138
logical interface 2-88

loopback error
detection for 2-64
recovery timer 2-66
loop guard, for spanning tree 4-23, 4-27

M

mac access-group command 2-140
MAC access-groups, displaying 3-101
MAC access list configuration mode 2-142
mac access-list extended command 2-142
MAC access lists 2-53
MAC addresses
disabling MAC address learning per VLAN 2-146
displaying
aging time 3-107
all 3-105
dynamic 3-113
MAC address-table move updates 3-118
notification settings 3-117, 3-120
number of addresses in a VLAN 3-111
per bridge domain 3-109
per interface 3-115
per VLAN 3-124
static 3-122
static and dynamic entries 3-103
dynamic
aging time 2-144
deleting 2-35
displaying 3-113
enabling MAC address notification 2-150
enabling MAC address-table move update 2-148
matching 2-160
static
adding and removing 2-152
displaying 3-122
dropping on an interface 2-152
tables 3-105
MAC address notification, debugging B-11
mac address-table aging-time 2-140, 2-160
mac address-table aging-time command 2-144
mac address-table learning command 2-146
mac address-table move update command 2-148
mac address-table notification command 2-150
mac address-table static command 2-152
macro description command 2-156
macro global command 2-157
macro global description command 2-159
macros
adding a description 2-156
adding a global description 2-159
applying 2-157
displaying 3-130
interface range 2-50, 2-90
specifying parameter values 2-157
tracing 2-157
maintenance end points 4-85
maps
class, creating 2-30
VLAN
creating 4-93
defining 2-160
displaying 3-157
match access-group command 2-162
match cos command 2-163
match discard-class command 2-165
match ip dscp command 2-166
match ip precedence command 2-168
match mpls experimental topmost command 2-170
match qos-group command 2-172
match vlan command 2-174
maximum transmission unit
See MTU
mdix auto command 2-179
memory (boot loader) command A-14
mgmt_clr (boot loader) command A-15
mgmt_init (boot loader) command A-16, A-17
mkdir (boot loader) command A-18

modes, commands 1-1
more (boot loader) command A-19
MPLS
displaying VFIs 3-152
experimental field 3-13
VCs 4-98
VFI configuration 2-127
MSTP
displaying 3-141
interoperability 2-39
link type 4-25
MST region
aborting changes 4-30
applying changes 4-30
configuration name 4-30
configuration revision number 4-30
current or pending display 4-30
displaying 3-141
MST configuration mode 4-30
VLANs-to-instance mapping 4-30
path cost 4-32
protocol mode 4-29
restart protocol migration process 2-39
root port
loop guard 4-23
preventing from becoming designated 4-23
restricting which can be root 4-23
root guard 4-23
root switch
affects of extended system ID 4-22
hello-time 4-35, 4-42
interval between BDPU messages 4-36
interval between hello BPDU messages 4-35, 4-42
max-age 4-36
maximum hop count before discarding BPDU 4-37
port priority for selection of 4-38
primary or secondary 4-42
switch priority 4-41
state changes
blocking to forwarding state 4-48
enabling BPDU filtering 4-14, 4-46
enabling BPDU guard 4-16, 4-46
enabling Port Fast 4-46, 4-48
forward-delay time 4-34
length of listening and learning states 4-34
rapid transition to forwarding 4-25
shutting down Port Fast-enabled ports 4-46
state information display 3-140
MTU, configuring size 2-181
mtu command 2-181
multicast router ports, configuring 2-112
multicast storm control 4-55
Multiple Spanning Tree Protocol
See MSTP
multiprotocol label switching
See MPLS

N

native VLANs 4-71
native VLAN tagging 4-95
neighbor command, VFI configuration mode 2-127
network-clock_select command 2-43, 2-45
network-clock hold-off command 2-182
network-clock input-source command 2-183
network clock priority 2-194
network-clock revertive command 2-185
network-clock-select command 2-188
network-clock-select hold-off timeout command 2-189
network-clock-select hold-timeout command 2-190
network-clock-select mode command 2-192
network-clock-select option command 2-193
network-clock-select output command 2-194
network-clock-select wait-to-restore command 2-195
network-clock synchronization ssm option command 2-186
network-clock wait-to-restore command 2-187

nonegotiate, speed 4-53
non-IP protocols
denying 2-53
forwarding 2-201
non-IP traffic access lists 2-142
non-IP traffic forwarding
denying 2-53
permitting 2-201
normal-range VLANs 4-90
no vlan command 4-90

O

OAM PDUs 2-72
OAM protocol 2-196
oam protocol cfm svlan command 2-196
on-board failure logging, displaying 3-97
on-board failure logging, enabling 2-86
online diagnostics
global configuration mode
clearing test-based testing schedule 2-56
setting test-based testing 2-56
setting up test-based testing 2-56
removing scheduling 2-56
scheduled switchover
disabling 2-56
enabling 2-56
scheduling 2-56
setting test interval 2-56
starting testing 2-58, 2-60
online diagnostic tests
displaying results 3-45
starting 2-58
operation, administration, and maintenance protocol
See OAM
output policy maps
and QoS group classification 2-172
and traffic shaping 3-24
configuration guidelines 2-209
queue limit in 2-217

P

pagp learn-method command 2-197
pagp port-priority command 2-199
password-recovery mechanism, enabling and disabling 3-4
peek (boot loader) command A-20
permit command 2-201
per-port per VLAN policing 2-174
per-VLAN spanning-tree plus
See STP
physical-port learner 2-197
PID, displaying 3-79
PIM-DVMRP, as multicast router learning method 2-112
ping (boot loader) command A-21
poke (boot loader) command A-22
police
multiple conform actions for a class 2-41
multiple exceed actions for a class 2-78
multiple violate actions for a class 4-88
police command 2-204
policers, configuring 2-204
policy-map class, configuring multiple actions 2-41, 2-78, 4-88
policy-map class configuration mode 2-28
policy-map class police configuration mode 2-41, 2-206
policy-map command 2-208
policy-map configuration mode 2-208
policy maps
and CoS classification 2-163
and DSCP classification 2-166
and IP precedence classification 2-169
and MPLS classification 2-170
applying 3-6
applying to an interface 3-6, 3-21
creating 2-208
displaying 3-132

policers 2-204
setting priority 2-214
setting QoS group identifier 3-19
traffic classification, defining 2-28
traffic marking
setting CoS values 3-8
setting DSCP values 3-11
setting IP precedence values 3-17
port-channel load-balance command 2-211
Port Fast, for spanning tree 4-48
port ranges, defining 2-34, 2-48, 2-50
ports, debugging B-17
port-type command 2-213
power information, displaying 3-49
power-supply status, displaying 3-49
precedence
for QoS traffic marking 3-17
setting in policy maps 3-17
priority command 2-214
privileged EXEC mode 1-2, 1-3
product identification information, displaying 3-79
PVST+
See STP

Q

ql-enabled rep-segment command 2-216
QoS
classification based on VLAN IDs 2-174
class maps
creating 2-30
defining the match criteria 2-163
displaying 3-34
conform actions, configuring 2-42
displaying statistics for 3-132
exceed actions, configuring 2-79
per-port, per-VLAN hierarchical policy maps 2-174
policy maps
applying to an interface 3-6, 3-21
creating 2-208
defining policers 2-204
displaying policy maps 3-132
setting CoS values 3-8
setting DSCP values 3-11
setting IP precedence values 3-17
setting QoS group identifier 3-19
traffic classifications 2-28
violate actions, configuring 4-89
QoS groups
as match criteria 2-172
classification 2-174
for QoS traffic classification 3-19
setting in policy maps 3-19
QoS match criteria
ACLs 2-162
CoS value 2-163
discard class value 2-165
DSCP value 2-166, 2-170, 2-174
precedence value 2-168
QoS group number 2-172
topmost MPLS experimemtal label 2-170
quality of service
See QoS
queue-limit command 2-217

R

rapid per-VLAN spanning-tree plus
See STP
rapid PVST+
See STP
receiving flow-control packets 2-80
recovery mechanism
causes 2-66
display 3-32, 3-52, 3-56
timer interval 2-67
rename (boot loader) command A-23
rep admin vlan command 2-233

rep block port command 2-234
rep lsl-age-timer command 2-237
rep preempt delay command 2-239
rep preempt segment command 2-241
rep segment command 2-242
rep stcn command 2-245
reserved-only command 2-247
reset (boot loader) command A-24
rmdir (boot loader) command A-25
rmon collection stats command 3-1
root guard, for spanning tree 4-23

S

scheduled switchover
  disabling 2-56
  enabling 2-56
scheduling diagnostic tests 2-56
sending flow-control packets 2-80
service instance command 3-2
service password-recovery command 3-4
service policy (policy-map class configuration) command 3-8
service-policy interface configuration command 3-6
set (boot loader) command A-26
set_param (boot loader) command A-29
set cos command 3-8
set discard-class command 3-10
set dscp command 3-11
set mpls command 3-13
set network-clocks command 3-15
set precedence command 3-17
set qos-group command 3-19
setup command 3-21
SFPs, displaying information about 3-79
shape average command 3-24
show access-lists command 3-26
show archive status command 3-29
show boot command 3-30
show class-map command 3-34
show controllers bits command 3-35
show controllers cpu-interface command 3-36
show controllers ethernet-controller command 3-38
show controller utilization command 3-43
show diagnostic command 3-45
show env command 3-49
show errdisable detect command 3-52
show errdisable flap-values command 3-54
show errdisable recovery command 3-56
show etherchannel command 3-58
show ethernet service evc command 3-61
show flowcontrol command 3-62
show interface rep command 3-74
show interfaces command 3-64
show interfaces counters command 3-71
show interfaces rep command 3-74
show interface transceivers command 3-76
show inventory command 3-79
show ipc command 3-86
show ip igmp profile command 3-80
show ip igmp snooping command 3-81
show ip igmp snooping groups command 3-83
show ip igmp snooping mrouter command 3-85
show ip sla standards command 3-86
show ip sla twamp session command 3-86
show lacp command 3-90
show location command 3-94
show logging onboard command 3-97
show mac access-group command 3-101
show mac address-table address command 3-105
show mac address-table aging time command 3-107
show mac address-table bridge-domain command 3-109
show mac address-table command 3-103
show mac address-table count command 3-111
show mac address-table dynamic command 3-113
show mac address-table interface command 3-115
show mac address-table learning command 3-117
show mac address-table move update command 3-118

show mac address-table notification command 3-120, B-13
show mac address-table static command 3-122
show mac address-table vlan command 3-124
show network-clocks command 3-126
show pagp command 3-128
show parser macro command 3-130
show policy-map command 3-132
show policy-map interface output fields 3-134
show port-type command 3-135
show rep topology command 3-137
show spanning-tree command 3-140
show storm-control command 3-146
show udld command 3-148
show version command 3-150
show vfi command 3-152
show vlan access-map command 3-157
show vlan command 3-154
show vlan command, fields 3-155
show vlan filter command 3-158
shutdown command 4-1
shutdown command, VFI configuration mode 2-127
shutdown vlan command 4-2
sleep (boot loader) command A-30
SNMP host, specifying 4-8
SNMP informs, enabling the sending of 4-4
snmp mib rep trap-rate command 4-3
snmp-server enable traps command 4-4
snmp-server host command 4-8
snmp trap mac-notification change command 4-12
SNMP traps
  enabling MAC address notification trap 4-12
  enabling the MAC address notification feature 2-150
  enabling the sending of 4-4
software images
  deleting 2-52
  downloading 2-7
  upgrading 2-7
  uploading 2-13
software version, displaying 3-150
spanning-tree bpdufilter command 4-14
spanning-tree bpduguard command 4-16
spanning-tree cost command 4-18
spanning-tree etherchannel command 4-20
spanning-tree extend system-id command 4-22
spanning-tree guard command 4-23
spanning-tree link-type command 4-25
spanning-tree loopguard default command 4-27
spanning-tree mode command 4-29
spanning-tree mst configuration command 4-30
spanning-tree mst cost command 4-32
spanning-tree mst forward-time command 4-34
spanning-tree mst hello-time command 4-35
spanning-tree mst max-age command 4-36
spanning-tree mst max-hops command 4-37
spanning-tree mst port-priority command 4-38
spanning-tree mst pre-standard command 4-40
spanning-tree mst priority command 4-41
spanning-tree mst root command 4-42
spanning-tree portfast (global configuration) command 4-46
spanning-tree portfast (interface configuration) command 4-48
spanning-tree port-priority command 4-44
Spanning Tree Protocol
  See STP
spanning-tree vlan command 4-50
speed command 4-53
SSH, configuring version 2-124
static-access ports, configuring 4-60
statistics, Ethernet group 3-1
storm-control command 4-55
STP
  counters, clearing 2-39
  debug messages, display
    MSTP B-25
    optimized BPDUs handling B-24
    spanning-tree activity B-21
    switch shim B-27, B-29

transmitted and received BPDUs B-23
EtherChannel misconfiguration 4-20
extended system ID 4-22
path cost 4-18
protocol modes 4-29
root port
loop guard 4-23
preventing from becoming designated 4-23
restricting which can be root 4-23
root guard 4-23
root switch
affects of extended system ID 4-22, 4-51
hello-time 4-50
interval between BDPU messages 4-50
interval between hello BPDU messages 4-50
max-age 4-50
port priority for selection of 4-44
primary or secondary 4-50
switch priority 4-50
state changes
blocking to forwarding state 4-48
enabling BPDU filtering 4-46
enabling BPDU guard 4-16, 4-46
enabling Port Fast 4-46, 4-48
enabling timer to recover from error state 2-66
forward-delay time 4-50
length of listening and learning states 4-50
shutting down Port Fast-enabled ports 4-46
state information display 3-140
VLAN options 4-41, 4-50
SVIs, creating 2-92
switching characteristics
modifying 4-58
returning to interfaces 4-58
switchport access command 4-60
switchport backup interface command 4-62
switchport block command 4-66
switchport command 4-58
switchport host command 4-68
switchport mode command 4-69
switchport port-security aging command 4-71
switchports, displaying 3-64
switchport trunk command 4-71
SyncE clock configuration 3-126
SyncE input clock 2-188
Synchronous Ethernet
See SyncE
system env temperature threshold yellow command 4-73
system message logging, save message to flash 2-138

T

tar files, creating, listing, and extracting 2-10
TDR, running 4-74
temperature information, displaying 3-49
temperature status, displaying 3-49
test cable-diagnostics tdr command 4-74
traceroute mac command 4-75
traceroute mac ip command 4-78
traffic shaping, QoS 3-24
trunking, VLAN mode 4-69
trunk mode 4-69
trunk ports 4-69
type (boot loader) command A-31

U

UDLD
aggressive mode 4-80, 4-82
debug messages, display B-35
enable globally 4-80
enable per interface 4-82
error recovery timer 2-66
message timer 4-80
normal mode 4-80, 4-82
reset a shutdown interface 4-84
status 3-148

udld command 4-80
udld port command 4-82
udld reset command 4-84
unicast storm control 4-55
uni count command 4-85
UniDirectional Link Detection
See UDLD
UNI ID, Ethernet 2-73
uni-vlan command 4-87
unknown multicast traffic, preventing 4-66
unknown unicast traffic, preventing 4-66
unset (boot loader) command A-32
upgrading software images
configuring 2-7
monitoring status of 3-29
user EXEC mode 1-2

V

VCs, assigning interfaces to 4-98
version (boot loader) command A-34
VFI
configuration mode commands 2-127
creating 2-127, 4-98
displaying 3-152
VPN ID for 4-97
violate-action command 4-88
virtual forwarding infrastructure
See VFI
virtual private networks
See VPNs
vlan access-map command 4-93
VLAN access map configuration mode 4-93
VLAN access maps
actions 2-2
displaying 3-157
vlan command 4-90
VLAN configuration mode
commands 4-90
description 1-4
entering 4-90
summary 1-2
vlan dot1q tag native command 4-95
vlan filter command 4-96
VLAN filters, displaying 3-158
VLAN ID range 4-90
VLAN maps
applying 4-96
creating 4-93
defining 2-160
displaying 3-157
VLANs
adding 4-90
configuring 4-90
debug messages, display
activation of B-33
VLAN IOS file system error tests B-32
VLAN manager activity B-31
displaying configurations 3-154
extended-range 4-90
MAC addresses
displaying 3-124
number of 3-111
normal-range 4-90
restarting 4-2
saving the configuration 4-90
shutting down 4-2
suspending 4-2
VPN
configuring 4-97
specifying in VFI configuration mode 2-127
vpn id command 4-97

W

Weighted Tail Drop
See WTD
WRED (Weighted Random Early Detection)

minimum threshold values (table) 2-232
WTD, queue-limit command 2-217

X

xconnect command 4-98